Department of Defense
Unified Capabilities Requirements 2010 (UCR 2010)

Final

January 2011

The Office of the Assistant Secretary of Defense
for
Networks and Information Integration / DoD Chief
Information Officer

DEPARTMENT OF DEFENSE
UNIFIED CAPABILITIES REQUIREMENTS 2010 (UCR 2010)

This document specifies technical requirements for certification of approved products supporting voice, video, and data applications services to be used in Department of Defense networks to provide end-to-end Unified Capabilities.

It conforms to Public Law 107-314 and is the basis for any future Unified Capabilities device acquisition, independent of the technology.

DISTRIBUTION STATEMENT A:
Approved for public release; distribution is unlimited.

SIGNATURE TO BE INSERTED HERE

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

SECTION 1
PURPOSE

1.1 The “Department of Defense Unified Capabilities Requirements 2010 (UCR 2010)” (hereinafter referred to as “UCR 2010”), specifies the technical requirements for certification of approved products to be used in Department of Defense (DoD) networks to provide end-to-end (E2E) Unified Capabilities (UC).

1.2 This document ~~augments~~ replaces UCR 2008, Change 1~~, dated 22 January 2009~~.

1.3 The UCR specifies the functional requirements, performance objectives, and technical specifications for DoD networks that support UC, and shall be used to support test, certification, acquisition, connection, and operation of these devices. It may also be used for UC product assessments and/or operational tests for emerging UC technology. DISA shall translate DoD Component functional requirements into engineering specifications for inclusion into the UCR, which shall identify the minimum requirements and features for UC applicable to the overall DoD community. The UCR shall also define interoperability, ~~IA~~Information Assurance, and interface requirements among products that provide UC. The ~~IA~~Information Assurance portion of the UC Test Plan (TP) shall be based on the requirements of the UCR as derived from Reference DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003

~~the functional requirements, performance objectives, and technical specifications for DoD networks that support UC. establishes the governing policy for UC products and services supported on DoD networks.~~

1.4 The UCR is based on COTS products’ features, Defense Information Systems Registry (DISR) and unique requirements needed to support DoD mission critical needs.

~~The UC benefits of leveraging emerging technologies to the warfighter include the following:~~

- ~~Global fixed and deployable E2E Interoperability over Internet Protocol (IP):~~
  - ~~Resolution of Interoperability, Information Assurance, and performance issues.~~
  - ~~Conducting DoD UC Operational Trial (Pilot) in Spirals.~~
- ~~Network Operations (NETOPS): Enables integrated network management (NM) for performance monitoring (PM) and situational awareness (SA).~~

~~– Enhanced situational assessments and information availability: Proliferation of IP-addressed sensors, munitions, biosensors, and logistics tracking applications.~~

~~• Voice and Video management consolidates at Defense Information Systems Agency (DISA) and Service Network Operations and Security Centers (NOSCs).~~

~~• Potential cost savings: Reduced footprint, personnel, training, and operations and maintenance costs.~~

~~• Integrated operations: Ubiquitous, robust, and scalable E2E networks.~~

~~• Information Assurance specifications: Establishes rigorous specifications and governance to reduce exposure to threats.~~

~~– New Information Assurance strategies that support mission assurance: E2E security, authentication, and non-repudiation.~~

~~• Increased operations tempo: Rapid reorganizational capabilities, shared SA, and improved wireless and mobility support.~~

~~• Greater support for communications on the move.~~

~~• Improved multicasting: Dynamic formation of communities of interest (COIs).~~

~~• Real-time collaboration: Integrated voice, video, and data capabilities.~~

~~• SA using NETOPS COI information sharing.~~

~~• Quicker, more dynamic responses: Rapid and agile Information Technology (IT) infrastructures with the capability to "discover" adjacent networks and plug-n-play.~~

~~• Provision of approved products for Combatant Commanders/Services/ Agencies (CC/S/As) to purchase.~~

SECTION 2
APPLICABILITY, DEFINITION, AND SCOPE

2.1 APPLICABILITY

The UCR applies to:

1. The Office of the Secretary of Defense (OSD), the Military Departments (MILDEPs), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (COCOMs), the Office of the Inspector General of the DoD, the defense agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

2. All equipment or software (hereinafter referred to as "UC products" or "products") and services that provide or support UC during each phase of those products' life cycles, from acquisition to operations, including:

   a. All UC products and end-to-end voice, video, and data services acquired or operated by the DoD Components or by authorized non-DoD users (e.g., combined or coalition partners and U.S. Government departments and agencies). Authorized non-DoD network users are required to comply with approved interfaces contained in Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)/DoD Chief Information Officer (DoD CIO) publication, "DoD Unified Capabilities Requirements (UCR)").

   b. All products and technologies used to send and receive or to support voice, video, or data across DoD networks that provide UC services.

   c. DoD Components' planning, investment, development, acquisition, operations, and management of DoD networks that provide UC services.

3. Th~~is~~e ~~Instruction~~UCR does NOT apply to:

(1) DoD Component acquisition programs governed by References (f) and (g) and Chairman of the Joint Chiefs of Staff Instruction 3170.01G (Reference (h)), except as stated in subparagraph a.(4) of this section; however, the DoD Components are encouraged to use UC-certified products in developing acquisition programs, where appropriate.

(2) DoD cryptologic Special Compartmented Information systems and classified cryptologic products, pursuant to DoDI 8500.2 (Reference (i)).

~~DoD Components' Programs of Record, specifically those governed by DoD Directive (DoDD) 5000.01, DoD Instruction (DoDI) 5000.02, and CJCS Instruction (CJCSI) 3170.01G are not subject to the provisions of this publication; however, are encouraged to use UC certified products in the development of programs, where appropriate~~.

2.2 UC DEFINITION

Unified Capabilities are the integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities~~Unified Capabilities are the integration of voice, video, and data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities. Unified Capabilities integrates standards-based communication and collaboration services including, but not limited to: messaging; voice, video, and web conferencing; and unified communication and collaboration applications or clients. These standards-based UC services are integrated with available enterprise applications, both business and warfighting~~.

2.3 SCOPE OF DOCUMENT

The UCR consists of the following seven sections:

1. Section 1, Purpose, for the UCR.

2. Section 2, Applicability, Definition, and Scope, of the UCR.

3. Section 3, Policy/Requirements, provides a broad overview of policies and requirements that will be implemented in the UCR with emphasis on policies and requirements that govern Information Assurance and Interoperability requirements and testing of products used to provide DoD UC.

4. Section 4, Unified Capabilities Mission Requirements, E2E Network Descriptions ~~Description and~~ Key Processes, ~~provides an overview of UC services and the core processes~~ needed for a vendor's product to gain placement on the DoD UC Approved Products List (APL).

5. Section 5, Unified Capabilities Product Requirements, describes technical requirements, features, and test configurations of equipment used to achieve approval to appear on the DoD UC APL. Section 5 also contains Change sheets that identify changes for which the 18-month rule applies.

6. Section 6 contains unique requirements: Section 6.1, Unique Requirements for Deployable Products, and Section 6.2, Unique Classified ~~VVoIP~~ UC Requirements.

7. Section 7, Product Categories Requirements Matrix, contains a high-level requirements matrix, which is a summary of the requirements defined in Sections 5 and 6 for the UC product categories and the products within those categories.

8. Appendix A, Definitions, Abbreviations and Acronyms, and References, contains the definitions, abbreviations, acronyms, and references applicable to the UCR.

Sections 1 through 4 are intended to serve as the summary of the UCR. Sections 5 and 6 are intended for product vendors and testers.

SECTION 3
POLICY/REQUIREMENTS

3.1 ~~INTRODUCTION~~UCR REQUIREMENT FRAMEWORK

~~This section provides a broad overview of policies that will be implemented in the UCR. The overview is focused on policies that govern Information Assurance and Interoperability verification and testing of systems and components used in providing UC. The UCR translates the mission-based requirements outlined by the major policies listed in Table 3.1-1, Major Policies Addressed by the UCR, into requirements that allow vendors to develop the functionality needed to meet those mission-based requirements, and for the DoD Distributed Test Laboratories to conduct the testing necessary to place those products on the DoD UC APL.~~

~~Table 3.1-1. Major Policies Addressed by UCR~~

~~DoDI 8100.ee, "Department of Defense Unified Capabilities," Draft, October 2009~~
~~DoDD 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005~~
~~DoDD 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009~~
~~DoDI 8100.3, "Department of Defense (DoD) Voice Networks," January 16, 2004 (hereby canceled)~~
~~ASD/(NII) Memorandum, "Department of Defense Unified Capabilities Requirements," current edition~~
~~DoDD 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004~~
~~DoDI 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004~~
~~DoDD 8500.01E "Information Assurance," October 24, 2002~~
~~DoDI 8500.2, "Information Assurance Implementation," February 6, 2003~~
~~DoDI 8510.01, "DoD Information Assurance (IA) Certification and Accreditation Process (DIACAP)," November 28, 2007~~
~~DoDI 8410.02, "DoD NETOPS for the Global Information Grid (GIG)," December 19, 2008~~

~~3.1.1 UC Policy Documents~~

This section provides a broad overview of requirements that establish the direction to be followed in the ~~UC MP~~UCR. The overview is focused on requirements for DoD Component planning, investment, development, acquisition, operations, and management of DoD networks that provide UC.

Unified Capabilities are the integration of voice, video, and data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities. Unified Capabilities integrate standards-based communication and collaboration services including, but not limited to, messaging; voice, video, and web conferencing; and unified communication and collaboration applications or clients. These standards-based UC services are integrated with available enterprise applications, both business and warfighting.

Implementation of UC across DoD is dependent on UC Transport, which is the secure and highly available enterprise network infrastructure used to provide voice, video, and data services through a combination of DoD and commercial terrestrial, wireless, and satellite communications (SATCOM) capabilities.

DoDI 8100.ee provides the policies that govern UC. However, certain policies are the primary drivers of UC migration in that they define the technology insertions and mission capability objectives that must be accomplished in specific timeframes.

Migration to UC is required to meet the requirements of the IP-enabled battlefield of the future. Unified Capabilities will allow DoD to achieve the following:

- Ubiquitous, robust, and scalable DoD networks, enabling integrated operations

- Proliferation of IP-addressed sensors, munitions, biosensors, and logistics tracking applications, which will enhance situational assessments and information availability

- End device to end device security, authentication, and non-repudiation, which will enable new Information Assurance strategies that support mission assurance

- Increased operations tempo supported by rapid reorganizational capabilities, shared situational awareness, and improved wireless and mobility support

- Greater support for communications on the move

- Dynamic formation of communities of interest (COIs) supported by improved multicasting

- Real time collaboration using integrated voice, video, and data capabilities

- Situational awareness using Network Operations (NETOPS) COI information sharing

- Rapid and agile information technology infrastructures with the capability to "discover" adjacent networks and plug and play to facilitate quicker, more dynamic responses

Figure 3-1 illustrates the relationships among the documents that provide the Requirements Framework for UC Migration and technology insertions.

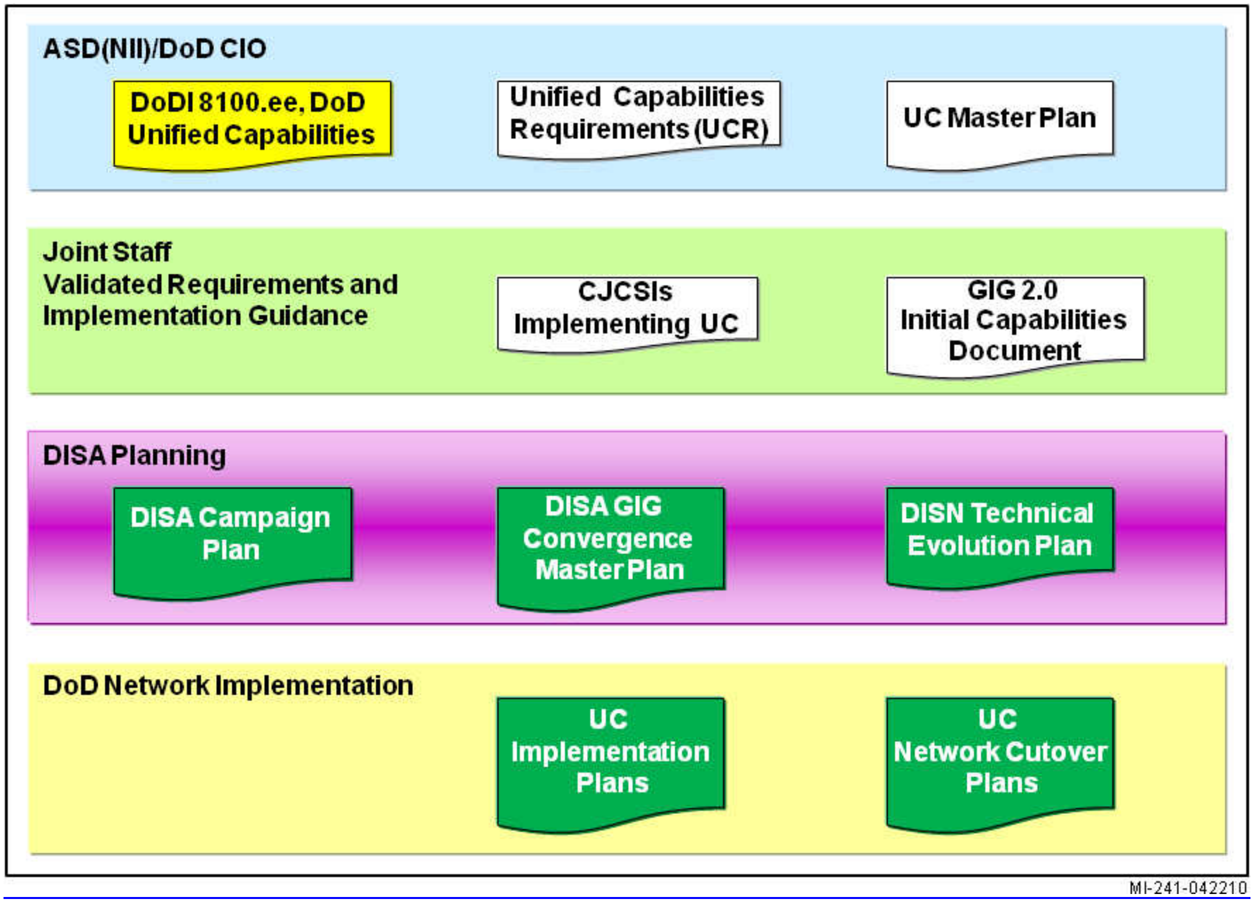

ASD(NII)/DoD CIO
DoDI 8100.ee, DoD Unified Capabilities
Unified Capabilities Requirements (UCR)
UC Master Plan
Joint Staff
Validated Requirements and Implementation Guidance
CJCSIs Implementing UC
GIG 2.0 Initial Capabilities Document
DISA Planning
DISA Campaign Plan
DISA GIG Convergence Master Plan
DISN Technical Evolution Plan
DoD Network Implementation
UC Implementation Plans
UC Network Cutover Plans
MI-241-042210

Figure 3-1. Requirements Framework for UC Migration and Technology Insertions

There are three key Assistant Secretary of Defense for Networks & Information Integration (ASD(NII))/DoD Chief Information Officer (CIO) documents that drive UC migration. The first is the DoDI 8100.ee, "DoD Unified Capabilities," which defines UC for the DoD; establishes policy, assigns responsibilities, and provides procedures for test, certification, acquisition, procurement, or lease (hereafter referred to as "acquisition"); effective, efficient, and economical transport, connection, and operation of DoD networks to provide UC; and establishes the governing policy for UC products and services supported on DoD networks.

The second ASD(NII)/DoD CIO document is the "Department of Defense Unified Capabilities Requirements," which specifies the technical requirements for certification of approved products to be used in DoD networks to provide UC. The third document is the “Department of Defense Unified Capabilities Master Plan (UC MP),” which synchronizes the migration investments in UC approved products across DoD networks to ensure mission performance is not degraded and enhanced mission capabilities are deployed in a timely manner.

Once the DoDI 8100.ee, “DoD Unified Capabilities,” is issued, Joint Staff will publish appropriate implementing instructions for UC. Global Information Grid 2.0 (GIG 2.0) has been initiated to meet warfighter requirements across the range of military operations. GIG 2.0 transforms the current understanding of the GIG from a federated set of systems, processes, governance, and control to a unified and integrated net-centric environment. To support this transformation the “Global Information Grid 2.0 (GIG 2.0) Initial Capabilities Document (ICD)” (hereafter referred to as “GIG 2.0 ICD”) (as approved in Joint Requirements Oversight Council Memorandum (JROCM) 095-09, dated 1 June 2009) is an overarching document identifying desired capabilities for the future of the GIG. GIG 2.0 is envisioned to fulfill the global requirements of the Combatant Command/Service/Agency (CC/S/A) communities and serves as a platform to implement the DoD Information Enterprise (IE). GIG 2.0 provides capabilities to all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites), and includes providing interfaces to coalition and mission partners, allies, and non-DoD users and systems. GIG 2.0 will facilitate mission support emanating from joint bases in support of the warfighter. GIG 2.0 also encompasses communications paths, such as MILSATCOM (Military Satellite), commercial SATCOM, and terrestrial gateway. The five GIG 2.0 ICD critical characteristics that must be met by UC migration are Global Authentication, Access Control, and Directory Services; Information and Services “from the Edge”; Joint Infrastructure; Common Policies and Standards; and Unity of Command. The five GIG 2.0 critical characteristics with the UC initiatives addressing them in parentheses are as follows:

- Global Authentication, Access Control, and Directory Services (UC Portable Assured Services in UC Pilots, UCR and UC Approved Products List (APL) Products)

- Information and Services “from the Edge” (UC Assured Quality Services to Deployed Tactical Units based on the UCR and UC APL Products)
- Joint Infrastructure (Technology Insertions and UC Spiral Demonstrations of NETOPS to Enable Information Sharing to Respond to Situational Awareness across a Diverse Spectrum of Operational Requirements)

- Common Policies and Standards (UCR and Test Programs for UC Spirals and for UC APL Products)

- Unity of Command (Technology Insertions and UC Spiral Demonstrations of NETOPS to Enable Information Sharing to Respond to Situational Awareness across a Diverse Spectrum of Operational Requirements)

DISA has three major planning documents that are both driving and supporting the UC planning activities. The first is the "DISA Campaign Plan," which identifies three "Lines of Operations," Enterprise Infrastructure, Command and Control (C2) and Information Sharing, and Operate and Assure with specific tasks that the UC Migration must support. The three "Lines of Operations" with the UC initiatives addressing them in parentheses are as follows:

- Enterprise Infrastructure (UCR, Technology Insertions and Test Programs for UC Spirals and for UC APL Products)

- Command and Control and Information Sharing (UCR, Assured and Secure Products, Technology Insertions and UC Spiral Demonstrations of NETOPS to Enable Information Sharing to Respond to Situational Awareness across a Diverse Spectrum of Operational Requirements)

- Operate and Assure (UCR, Assured and Secure Products, Technology Insertions and UC Spiral Demonstrations of NETOPS to Enable Information Sharing to Respond to Situational Awareness across a Diverse Spectrum of Operational Requirements)

The second document is the "DISA Global Information Grid (GIG) Convergence Master Plan," which identifies five categories of DISA programs: Application, Services, and Data; Communications and Networks; Information Assurance; Network Operations and Enterprise Management; and Computing Infrastructure. These DISA programs and their migration directly affect the UC migration. The five categories with the UC initiatives addressing them in parentheses are as follows:

- Applications, Services, and Data (UC Collaboration Services Non-Assured Services with Quality of Service (QoS) and Assured Services with QoS)

- Communications and Networks (UC Assured Services via UCR and UC APL Products)
- Information Assurance (End-to-End Information Assurance UCR and Information Assurance Governance)

- NETOPS and Enterprise Management (NETOPS Concept of Operations (CONOPS)/Joint Tactics, Techniques, and Procedures (JTTPs), UC Element Management Systems (EMS))

The third document is the "Defense Information System Network (DISN) Technical Evolution Plan (DTEP)." The DTEP addresses "how" and "when" for the DISN UC technical migration. The DTEP includes a section on DISN UC evolution and a section on DISN UC deployment, which addresses the technology migrations outlined in the "DoD Unified Capabilities Requirements (UCR)." The UC MP is consistent with these DISN documents, as well as DoD Components' UC technology implementation plans. The DTEP four key capabilities with the UC initiatives addressing them in parentheses are as follows:

- Information Assurance (Information Assurance Technical Requirements in the UCR and Information Assurance Governance)
- Connectivity (Assured Services Requirements in the UCR)
- Network Management (NETOPS CONOPS/JTTPs, UC EMS)
- Interoperability (UCR and Test Programs for UC Spirals and for UC APL Products)

There are two documents essential to synchronizing investments across DoD by the Defense Information Systems Agency (DISA) and other DoD Components. These documents are the UC implementation plans, and the UC Network Cutover Plans (NCPs). The UC MP defines three spiral timeframes (i.e., near-, mid-, and far-term) to be used as context for DoD Components' POM actions. The UC implementation plans synchronize the deployment of UC from a DoD networks perspective based on DoD Components' acquisition plans by quarter of fiscal year (FY). The UC NCPs ensure the readiness of UC site installations, UC Transport and Network Operations and Security Centers (NOSCs) as they become operational.

The most demanding set of requirements in these documents are those associated with the following:

- Information Assurance consistent with the DoD Information Assurance Certification and Accreditation Process (DIACAP) and Security Technical Implementation Guides (STIGs) that must change constantly due to emerging vulnerabilities and threats
- Assured services across hybrid circuit-switched and IP networks
- End-to-end Interoperability among multiple vendors
- End-to-end Interoperability between fixed and multiple deployable programs
- NETOPS: Performance: Sustaining high QoS for end-to-end voice, video, collaboration, and data performance over IP networks

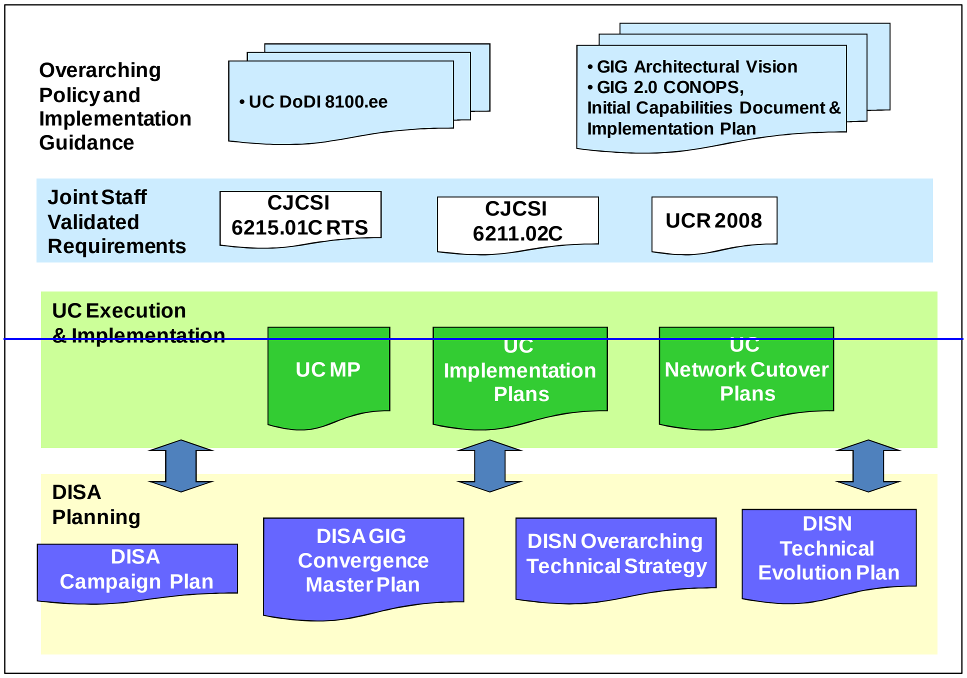
- NETOPS response to situational awareness: collaboratively adapting DoD networks via the command hierarchy to meet mission needs

- Internet Protocol Version 6 (IPv6) end device to end device performance leveraging the capabilities of IPv6

- Fully leveraging Commercial Off-the-Shelf (COTS) features associated with UC to enhance mission and combat support productivity

These requirements are the most demanding, because IP-based technologies have inherent Information Assurance limitations that must be mitigated, and they were not designed originally for the voice and video subset of UC services, and so, require a variety of techniques to support UC services properly. Thus, IP-based technologies require GIG Enterprise Wide Systems Engineering (EWSE) by the Government, development by industry, and test and evaluation by the Government to satisfy the policies and meet the requirements. In addition, the challenges and military services funding limitations force the installation of a common IP technology base to occur over a number of FYs. Thus, networks based on hybrid technologies including a mix of technologies (e.g., circuit-switched and/or IP), and converged or non-converged solutions, will be required for many years. The UC Deployment Spirals have been structured to resolve these challenges and to result in approved products for the DoD Components to purchase.

~~Figure 3.1.1-1, UC Policy and Technical Reference Documents, illustrates the relationships among the documents that drive, execute, and implement UC migration and technology insertions.~~


Overarching Policy and Implementation Guidance
• UC DoDI 8100.ee
• GIG Architectural Vision
• GIG 2.0 CONOPS, Initial Capabilities Document & Implementation Plan
Joint Staff Validated Requirements
CJCSI 6215.01C RTS
CJCSI 6211.02C
UCR 2008
UC Execution & Implementation
UC MP
UC Implementation Plans
UC Network Cutover Plans
DISA Planning
DISA Campaign Plan
DISA GIG Convergence Master Plan
DISN Overarching Technical Strategy
DISN Technical Evolution Plan

~~Figure 3.1.1-1. UC Policy and Technical Reference Documents~~

~~The overarching policy and implementation guidance for UC is provided by the ASD(NII)/DoD CIO "Global Information Grid (GIG) Architectural Vision" (hereinafter referred to as "GIG Architectural Vision") and the Joint Staff "Global Information Grid 2.0 (GIG 2.0) Concept of Operations (CONOPS)" (hereinafter referred to as "GIG 2.0 CONOPS")and "Global Information Grid 2.0 (GIG 2.0) Initial Capabilities Document (ICD)," (hereinafter to as "GIG 2.0 ICD") and the "GIG 2.0 Implementation Plan" (hereinafter referred to as "GIG 2.0 Implementation Plan"). The major drivers of UC migration are the DoD objective enterprise architecture as defined by the "GIG Architectural Vision" and the Joint Staff-validated strategic requirements in the "GIG 2.0 ICD." This objective enterprise architecture is driven by emerging IP and changing communications technologies, which recognizes evolving communication capabilities from point-to-point to multipoint, voice-only to rich-media, multiple devices to a single device, wired to wireless, non-real time to real time, and scheduled to ad hoc.~~

~~The following five GIG 2.0 critical characteristics with the UC initiatives addressing them in parentheses are as follows:~~

- ~~Global Authentication, Access Control, and Directory Services (UC Portable Assured Services in UC Pilots, UCR and APL Products)~~

- ~~Information and Services "from the Edge" (UC Assured Services to Deployed Tactical Units Based on the UCR and APL Products)~~

- ~~Joint Infrastructure (NETOPS to Enable Information Sharing across a Diverse Spectrum of Operational Requirements)~~
- ~~Common Policies and Standards (UCR and Test Programs for UC Spirals and for APL Products)~~

- ~~Unity of Command (NETOPS for UC Response to Situational Awareness)~~

~~Joint Staff-validated requirements for Real Time Services (RTS), which are critical UC, are initially addressed in CJCSI 6215.01C, "Policy for Department of Defense (DoD) Voice Networks with Real Time Services (RTS)." CJCSI 6211.02C, "DISN: Policy and Responsibilities," provides the connection approval processes for the Defense Information System Network (DISN), and is applicable to UC within the DISN. The ASD(NII)/DoD CIO document, "DoD Unified Capabilities Requirements (UCR) 2008," contains the first comprehensive Joint Staff-validated requirements for UC.~~

~~Unified Capabilities execution and implementation documents essential to synchronizing investments across DoD by the DISA and other DoD Components are the UC MP, the UC implementation plans, and the UC network cutover plans (NCPs). The UC MP defines three~~

~~spiral timeframes (i.e., near-, mid-, and far-term) to be used as context for DoD Components' Program Objective Memorandum (POM) actions. The UC implementation plans synchronize the deployment of UC based on DoD Components' acquisition plans by fiscal year (FY) quarter. The UC NCPs ensure the readiness of UC site installations as they become operational.~~

~~DISA has four major planning documents that are both driving and supporting the UC planning activities. The first is the "DISA Campaign Plan," which identifies areas of focus with the UC initiatives addressing them in parentheses as follows:~~

- ~~Enterprise Infrastructure (UCR and Test Programs for UC Spirals and for APL Products)~~
- ~~Command and Control and Information Sharing (UCR and NETOPS)~~
- ~~Operate and Assure (NETOPS and APL Products)~~

~~The second document is the DISA GIG Convergence Master Plan (DGCMP) that identifies four categories with the UC initiatives addressing them in parentheses as follows:~~

- ~~Applications, Services, and Data (UC Collaboration Services Non-Assured Services (AS) with Quality of Service (QoS) and AS with QoS)~~
- ~~Communications/Networks (UC E2E Assured Services via UCR and APL Products)~~
- ~~Information Assurance (E2E Information Assurance UCR and Information Assurance Governance)~~
- ~~NETOPS/Enterprise Management (NETOPS CONOPS/Joint Tactics, Techniques and Procedures (JTTPs), RTS Element Management System (EMS)/Probes)~~

~~The third and fourth documents are the "DISN Overarching Technical Strategy (DOTS)" and the "DISN Technology Evolution Plan (DTEP)," shown in Figure 3.1-1, UC Policy and Technical Reference Documents. The DOTS addresses "what" DISA is doing from a technology perspective for DISN. The DTEP addresses "how" and "when" for the DISN UC technical migration. The DTEP includes a section on DISN UC evolution and a section on DISN UC deployment. Both documents address the technology migrations outlined in the "DoD Unified Capabilities Requirements (UCR)." The "UC MP" is consistent with these DISN documents, as well as DoD Components' UC technology implementation plans. The DOTS and the DTEP identify four key capabilities with the UC initiatives addressing them in parentheses as follows:~~

- ~~Information Assurance (E2E Information Assurance UCR and Information Assurance Governance)~~
- ~~Connectivity (UCR)~~
- ~~Network Management (NETOPS CONOPS/JTTPs, RTS EMS/Probes)~~
- ~~Interoperability (UCR and Test Programs for UC Spirals and for APL Products)~~

3.2 MISSION CAPABILITIES

Assured Services Features (ASFs) must be provided by UC networks based on the mission of the users consistent with their roles in peacetime, crisis, and war. There are users who need the full range of assured services, those that only need limited assured services, and those that need non-assured services. Even if requirements for assured services do not apply to all users at a site the Assured Information Protection features cannot be degraded.

In the operation of networks that provide UC services, the DoD Components shall comply with ASFs requirements, i.e., Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery) defined as follows:

1. Assured System and Network Availability. Achieved through visibility and control over the system and network resources. Resources are managed and problems are anticipated and mitigated, ensuring uninterrupted availability and protection of the system and network resources. This includes providing for graceful degradation, self-healing, failover, diversity, and elimination of critical failure points. This ASF supports user traffic during peacetime, crisis, conflict, natural disaster, and network disruptions, and possesses the robustness to provide a surge capability when needed.

2. Assured Information Protection. Applies to information in storage, at rest, and passing over networks, from the time it is stored and catalogued until it is distributed to the users, operators, and decision makers. Secure end devices shall be used for the protection of classified and sensitive information being passed to ensure its confidentiality, integrity, and authentication. The DoD networks that provide UC services shall be configured to minimize attacks on the system that could result in denial or disruption of service. All hardware and software in the network must be Information Assurance certified and accredited.

3. Assured Information Delivery. The requirement that DoD networks providing UC services have the ability to optimize session completion rates despite degradation due to network disruptions, natural disasters, or surges during crisis or war.

3.2.1 Assured Services Features

This section provides more specific mission capabilities associated with the three UC Assured Services of Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery. The DoD UC networks and services shall have the following ASF to provide these three UC Assured Services:

1. Assured System and Network Availability. Supports mission critical traffic during peacetime, crisis, conflict, natural disaster, and network disruptions and possesses the robustness to provide a surge capability when needed. The following objectives contribute to the survivability of the UC:

    a. No single point of vulnerability for the entire network, to include the NM facilities. No single point of vulnerability within a COCOM-defined geographic region of the COCOM's theater.

    b. No more than 15 percent of the bases, posts, camps, or stations (B/P/C/Ss) within a COCOM-defined geographic region of the COCOM's theater can be affected by an outage in the network.

    c. Networks robustness through maximum use of alternative routing, redundancy, and backup.

    d. To the maximum extent possible, transport supporting major installations (i.e., B/P/C/S, leased or commercial sites or locations) will use physically diverse routes.

    e. The National Military Command Center (NMCC) (and Alternate), COCOMs, or DoD Component headquarters will not be isolated longer than 30 minutes because of an outage in the backbone (long-haul) portion of the network.

2. Assured Information Protection.

    a. Secure EIs (SEIs) shall be used for the protection of classified and sensitive information being passed to ensure its confidentiality, integrity, and authentication.

    b. The UC networks shall be configured to minimize and protect against attacks that could result in denial or disruption of service.

c. All hardware and software in the network must be Information Assurance certified and accredited and operated in accordance with (IAW) the most current Security Technical Implementation Guides (STIGs).

3. Assured Information Delivery.

a Assured connectivity ensures the connectivity from user instrument-to-user instrument across all DoD UC networks, including U.S. Government-controlled UC network infrastructures, achieved under peacetime, crisis, and war situations.

b. The DoD UC networks are required to provide precedence based assured services (PBAS) for delivery of UC services. Precedence based assured services (PBAS) requires the ability of the DoD UC networks to optimize session completion rates and, in some cases, prevent blocking of all mission-critical users' sessions despite degradation because of network disruptions, natural disasters, or surges during crisis or war. The DoD UC networks shall be designed with the capability to assign and reallocate resources on demand consistent with mission precedence. For voice and video sessions, PBAS shall allow higher precedence users to be provided with resources that had been allocated to lower precedence sessions. The PBAS is not required in the wide area network (WAN). Five precedence levels shall be provided. They are FLASH OVERRIDE (FO), FLASH (F), IMMEDIATE (I), PRIORITY (P), and ROUTINE (R). Authorization for origination of sessions that use these precedence levels to support mission-critical sessions shall be determined by the Joint Staff and COCOMs. All users shall be capable of receiving precedence UC services sessions since locations of crises and wars cannot be determine in advance.

c. Unified Capabilities services must be responsive to the needs of FLASH and FLASH OVERRIDE sessions, that are provided nonblocking service (i.e., P.00 threshold) from user to user. (NOTE: P.00 is the probability that out of every 100 calls, the probability is that zero sessions will be blocked.)

d. Precedence-based sessions placed to EIs that are busy with lower precedence-based sessions shall be absolutely assured completion to a live person. This shall be accomplished by immediate disconnection of the lower precedence session and immediate completion of the higher precedence session.

e. Visibility and Rapid Reconfiguration. If blocking occurs to users' sessions caused by crisis surge traffic, the network shall be rapidly reconfigurable to assign resources consistent with the response to SA to ensure minimal blocking to services critical to the response. Both DISA and the military services shall provide around-the-clock network operations centers (NOCs) that oversee voice, video, and data services. DISA shall oversee the DISN systems and shall have read-write access to DISN systems, which are shared with the military services for cost avoidance, such as the multifunction softswitch (MFSS) or WAN Softswitch (SS). All NOCs shall have EMSs that allow for read-write access for the systems for which they have direct responsibility. In addition, the Joint Task Force – Global Network Operations (JTF GNO)-sponsored NETOPS COI metadata standards and information sharing capabilities shall be used by all NOCs to share alarms, performance data, and trouble tickets. Information sharing shall allow for providing visibility E2E and for modifying the configuration of network components, as needed, to respond to SA. All actions shall be coordinated with DoD Components affected before such actions are taken, if possible, consistent with the "Operational Tempo" and after such actions are taken.

f. Mitigation of blocking of sessions that occur during short-term traffic surges shall be accomplished via PBAS.

g. During times of surge or crisis, the CJCS can direct implementation of session controls to allocate the use of resources in the network to meet mission needs.

h. The global and theater networks must be able to support a regional crisis in one theater, yet retain the surge capability to respond to a regional crisis occurring nearly simultaneously in another theater.

i. Unified Capabilities networks shall be designed with the capability to permit interconnection and interoperation with similar Services' deployable programs, U.S. Government, allied, and commercial networks. All hardware and software in the network must be certified as interoperable.

j. Unified Capabilities networks shall be designed to assure that E2E voice, video, and data performance are clear, intelligible, not distorted or degraded, using commercial standards performance metrics. The DoD UC networks shall be designed to meet voice, video, and data performance requirements E2E. Deployed UC networks can provide degraded performance consistent with meeting mission needs as compared to fixed UC network performance.

k. Non Assured voice and video flows shall be policed or controlled to ensure they do not degrade the performance of assured voice and video flows that are using PBAS.

SECTION 4
UNIFIED CAPABILITIES DESCRIPTION AND KEY PROCESSES

4.1 OVERVIEW

This section describes UC services, E2E UC network designs, the UC products that support those designs, and the core processes needed for a vendor to gain placement of its UC products on the DoD UC APL. Use of products from the DoD UC APL allows DoD Components to purchase and operate UC products over all DoD network infrastructures. This section applies to both fixed and deployable products that support UC services on DoD networks.

4.2 UNIFIED CAPABILITIES SERVICES DESCRIPTION

The major drivers of mission needs for UC services are addressed in Section 3. ~~the DoD objective enterprise architecture as defined by the "GIG Architectural Vision" and the Joint Staff-validated requirements in the "GIG 2.0 ICD."~~ UC services are ~~This objective enterprise architecture is~~ driven by emerging IP and changing communications technologies, which recognizes evolving communication capabilities from point-to-point to multipoint, voice-only to rich-media, multiple devices to single device, wired to wireless, non-real time to real time, and scheduled to ad hoc.

Assured UC services are required to meet the requirements of the IP-enabled battlefield of the future. Unified Capabilities will allow the DoD to achieve the following:

- Ubiquitous, robust, and scalable E2E networks, enabling integrated operations.
- Proliferation of IP-addressed sensors, munitions, biosensors, and logistics tracking applications, which will enhance situational assessments and information availability.
- End-to-end security, authentication, and non-repudiation, which will enable new Information Assurance strategies that support mission assurance.
- Increased operations tempo supported by rapid reorganizational capabilities, shared SA, and improved wireless and mobility support.
- Greater support for communications on the move.
- Dynamic formation of COIs supported by improved multicasting.

- Real-time collaboration using integrated voice, video, and data capabilities.
- SA using NETOPS COI information sharing.
- Rapid and agile IT infrastructures with the capability to “discover” adjacent networks and plug-n-play to facilitate quicker, more dynamic responses.

~~Unified Capabilities~~ Voice, video and data services that are addressed for integration in the UCR are as follows:

1. Voice and Video Services Point-to-Point. Provides for two voice and/or video users to be connected end instrument (EI)-to-EI with services that can include capabilities such as voice mail, call forwarding, call transfer, call waiting, operator assistance, and local directory services.

2. Voice Conferencing. Provides for multiple voice users to conduct a collaboration session.

3. Video Teleconferencing (VTC). Provides for multiple video users to conduct video and voice collaboration with a variety of room controls for displays of the participants often with a variety of scheduling tools.

4. E-Mail/Calendaring. Provides for users to send messages to one or many recipients with features such as priority marking, reports on delivery status and delivery receipts, digital signatures, and encryption. Calendaring allows the scheduling of appointments with one or many desired attendees.

5. Unified Messaging. Provides access to voice mail via e-mail or access to e-mail via voice mail.

6. Web Conferencing and Web Collaboration. Provides for multiple users to collaborate with voice, video, and data services simultaneously using web page type displays and features.

7. Unified Conferencing. Provides for multiple users to collaborate with voice, web, or videoconferencing integrated into a single, consolidated solution often as a collaboration application.

8. Instant Messaging (IM) and Chat. Provides real-time interaction among two or more users who must collaborate to accomplish their responsibilities using messages to interact when they are jointly present on the network. For IM, presence is displayed.

a. Instant messaging provides the capability for users to exchange one-to-one ad hoc text message over a network in real time. This is different and not to be confused with signal or equipment messaging, in that IM is always user generated and user initiated.

b. Chat provides the capability for two or more users operating on different computers to exchange text messages in real time. Distinguished from IM by being focused on group chat, or room-based chat. Typically, room persistence is a key feature of multiuser chat; in contrast with typically ad hoc IM capabilities.

c. Presence/Awareness is a status indicator that conveys ability and willingness of a potential user to communicate.

9. Rich-Presence Services. Allows contact to be achieved to individuals based on their availability as displayed by presence information from multiple sources, including IM, telephone, and mobile devices.

10. Mobility. Provides the ability to offer wireless and wired access, and applies to voice, e-mail, and many other communication applications. It includes devices such as personal digital assistants (PDAs) and smart telephones. In addition, it provides for users who move to gain access to enterprise services at multiple locations (e.g., your telephone number and desktop follow you).

Each of these UC services need to be provided by networks that meet E2E performance standards for QoS, which are defined in Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, for all DoD networks.

~~4.3 MISSION CAPABILITIES~~

~~Assured Services Features (ASFs) must be provided by UC networks based on the mission of the users consistent with their roles in peacetime, crisis, and war. There are users who need the full range of assured services, those that only need limited assured services, and those that need non-assured services. Even if requirements for assured services do not apply to all users at a site the Assured Information Protection features cannot be degraded.~~

~~In the operation of networks that provide UC services, the DoD Components shall comply with ASFs requirements, i.e., Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery) defined as follows:~~

~~1. Assured System and Network Availability. Achieved through visibility and control over the system and network resources. Resources are managed and problems are anticipated and mitigated, ensuring uninterrupted availability and protection of the system and network resources. This includes providing for graceful degradation, self-healing, failover, diversity, and elimination of critical failure points. This ASF supports user traffic during peacetime, crisis, conflict, natural disaster, and network disruptions, and possesses the robustness to provide a surge capability when needed.~~

~~2. Assured Information Protection. Applies to information in storage, at rest, and passing over networks, from the time it is stored and catalogued until it is distributed to the users, operators, and decision makers. Secure end devices shall be used for the protection of classified and sensitive information being passed to ensure its confidentiality, integrity, and authentication. The DoD networks that provide UC services shall be configured to minimize attacks on the system that could result in denial or disruption of service. All hardware and software in the network must be Information Assurance certified and accredited.~~

~~3. Assured Information Delivery. The requirement that DoD networks providing UC services have the ability to optimize session completion rates despite degradation due to network disruptions, natural disasters, or surges during crisis or war.~~

~~4.3.1 ASSURED SERVICES FEATURES~~

~~This section provides more specific mission capabilities associated with the three UC Assured Services of Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery. The DoD UC networks and services shall have the following ASF to provide these three UC Assured Services:~~

~~1. Assured System and Network Availability. Supports mission critical traffic during peacetime, crisis, conflict, natural disaster, and network disruptions and possesses the robustness to provide a surge capability when needed. The following objectives contribute to the survivability of the UC:~~

~~a. No single point of vulnerability for the entire network, to include the NM facilities. No single point of vulnerability within a COCOM-defined geographic region of the COCOM's theater.~~

~~b. No more than 15 percent of the bases, posts, camps, or stations (B/P/C/Ss) within a COCOM-defined geographic region of the COCOM's theater can be affected by an outage in the network.~~

~~**C. NETWORKS ROBUSTNESS THROUGH MAXIMUM USE OF ALTERNATIVE ROUTING, REDUNDANCY, AND BACKUP.**~~

~~**D. TO THE MAXIMUM EXTENT POSSIBLE, TRANSPORT SUPPORTING MAJOR INSTALLATIONS (I.E., B/P/C/S, LEASED OR COMMERCIAL SITES OR LOCATIONS) WILL USE PHYSICALLY DIVERSE ROUTES.**~~

~~**E. THE NATIONAL MILITARY COMMAND CENTER (NMCC) (AND ALTERNATE), COCOMS, OR DOD COMPONENT HEADQUARTERS WILL NOT BE ISOLATED LONGER THAN 30 MINUTES BECAUSE OF AN OUTAGE IN THE BACKBONE (LONG-HAUL) PORTION OF THE NETWORK.**~~

~~**2. ASSURED INFORMATION PROTECTION.**~~

~~**A. SECURE EIS (SEIS) SHALL BE USED FOR THE PROTECTION OF CLASSIFIED AND SENSITIVE INFORMATION BEING PASSED TO ENSURE ITS CONFIDENTIALITY, INTEGRITY, AND AUTHENTICATION.**~~

~~**B. THE UC NETWORKS SHALL BE CONFIGURED TO MINIMIZE AND PROTECT AGAINST ATTACKS THAT COULD RESULT IN DENIAL OR DISRUPTION OF SERVICE.**~~

~~**C. ALL HARDWARE AND SOFTWARE IN THE NETWORK MUST BE INFORMATION ASSURANCE CERTIFIED AND ACCREDITED AND OPERATED IN ACCORDANCE WITH (IAW) THE MOST CURRENT SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGS).**~~

~~3. ASSURED INFORMATION DELIVERY.~~

~~A ASSURED CONNECTIVITY ENSURES THE CONNECTIVITY FROM USER INSTRUMENT-TO-USER INSTRUMENT ACROSS ALL DOD UC NETWORKS, INCLUDING U.S. GOVERNMENT-CONTROLLED UC NETWORK INFRASTRUCTURES, ACHIEVED UNDER PEACETIME, CRISIS, AND WAR SITUATIONS.~~

~~b. The DoD UC networks are required to provide precedence based assured services (PBAS) for delivery of UC services. Precedence based assured services (PBAS) requires the ability of the DoD UC networks to optimize session completion rates and, in some cases, prevent blocking of all mission-critical users' sessions despite degradation because of network disruptions, natural disasters, or surges during crisis or war. The DoD UC networks shall be designed with the capability to assign and reallocate resources on demand consistent with mission precedence. For voice and video sessions, PBAS shall allow higher precedence users to be provided with resources that had been allocated to lower precedence sessions. The PBAS is not required in the wide area network (WAN). Five precedence levels shall be provided. They are FLASH OVERRIDE (FO), FLASH (F), IMMEDIATE (I), PRIORITY (P), and ROUTINE (R). Authorization for origination of sessions that use these precedence levels to support mission-critical sessions shall be determined by the Joint Staff and COCOMs. All users shall be capable of receiving precedence UC services sessions since locations of crises and wars cannot be determine in advance.~~

~~c. Unified Capabilities services must be responsive to the needs of FLASH and FLASH OVERRIDE sessions, that are provided nonblocking service (i.e., P.00 threshold) from user to user. (NOTE: P.00 is the probability that out of every 100 calls, the probability is that zero sessions will be blocked.)~~

~~d. Precedence-based sessions placed to EIs that are busy with lower precedence-based sessions shall be absolutely assured completion to a live person. This shall be accomplished by immediate disconnection of the lower precedence session and immediate completion of the higher precedence session.~~

~~e. Visibility and Rapid Reconfiguration. If blocking occurs to users' sessions caused by crisis surge traffic, the network shall be rapidly reconfigurable to assign resources consistent with the response to SA to ensure minimal blocking to services critical to the response. Both DISA and the military services shall provide around-the-clock network operations centers (NOCs) that oversee voice, video, and data services. DISA shall oversee the DISN systems and shall have read-write access to DISN systems, which are shared with the military services for cost avoidance, such as the multifunction softswitch (MFSS) or WAN Softswitch (SS). All NOCs shall have EMSs that allow for read-write access for the systems for which they have direct responsibility. In addition, the Joint Task Force – Global Network Operations (JTF GNO)-sponsored NETOPS COI metadata standards and information sharing capabilities shall be used by all NOCs to share alarms, performance data, and trouble tickets. Information sharing shall allow for providing visibility E2E and for modifying the configuration of network components, as needed, to respond to SA. All actions shall be coordinated with DoD Components affected before such actions are taken, if possible, consistent with the "Operational Tempo" and after such actions are taken.~~

~~f. Mitigation of blocking of sessions that occur during short-term traffic surges shall be accomplished via PBAS.~~

~~g. During times of surge or crisis, the CJCS can direct implementation of session controls to allocate the use of resources in the network to meet mission needs.~~

~~h. The global and theater networks must be able to support a regional crisis in one theater, yet retain the surge capability to respond to a regional crisis occurring nearly simultaneously in another theater.~~

~~i. Unified Capabilities networks shall be designed with the capability to permit interconnection and interoperation with similar Services' deployable programs, U.S. Government, allied, and commercial networks. All hardware and software in the network must be certified as interoperable.~~

~~j. Unified Capabilities networks shall be designed to assure that E2E voice, video, and data performance are clear, intelligible, not distorted or degraded, using commercial standards performance metrics. The DoD UC networks shall be designed to meet voice, video, and data performance requirements E2E. Deployed UC networks can provide degraded performance consistent with meeting mission needs as compared to fixed UC network performance.~~

4.3~~4~~ MIGRATION TO UNIFIED CAPABILITIES

The DoD “UC MP” provides the details on the migration to UC services. This section provides an overview of that migration to assist the DoD Components acquisition organizations and product vendors in understanding how the products will be used to meet mission needs.

The purpose of the “UC MP” is to

1. Define DoD’s migration from the current legacy technologies to converged net-centric, IP-based voice, video, and data services.

2. Serve as a guideline to the DoD Components in the preparation of migration and acquisition plans for phasing out circuit-switched voice and video services and initially phasing in Voice and Video over IP (VVoIP) services, and other UC services that will operate in converged voice, video, and data networks. The “UC MP” addresses synchronization of life-cycle activities, from acquisition to operations, for networks that provide UC services.

3. Provide guidance for DoD Components’ POM submissions.

The challenges of UC migration and DoD Component budgets prevent the ability to install a common IP technology base as a global “flash cut.” Thus, networks based on hybrid technologies will be required for many years. The DISN Evolution Spirals (see Figure 4.4-1, DISN Evolution Spirals) have been structured to address these challenges.

The DoD UC migration strategy must be integrated with DISN and DoD Component implementation planning to sustain E2E capabilities in a hybrid technology environment. The “UC MP” is structured to synchronize the DoD Components’ migration to E2E voice, video, and data services as rapidly as resources allow, consistent with respective business cases and mission needs.

To support timely UC implementation, the migration strategy is structured to fully leverage DISN technical refreshment investments. The “UC MP” is based on the DISN Spiral timeframes to synchronize DISN and DoD Components investments. Figure 4.4-1, DISN Evolution Spirals, illustrates the Near-Term, Mid-Term, and Far-Term DISN Spirals that depict the evolution to the target capabilities and infrastructure. These three Spirals are as follows:

- Near-Term (Current~~FY 2008~~–2012) – Circuit-Switched to IP Convergence
- Mid-Term (FY 2013–2016) – Voice, Video, and Data to Shared IP Convergence
- Far-Term (FY 2017–2020) – Multiple Classifications to Unified IP Convergence

At the completion of each Spiral, UC services are implemented, both by the DoD Components and in the DISN infrastructure. As shown in Figure 4.4-1, network-oriented capabilities will evolve to enhanced service oriented capabilities.

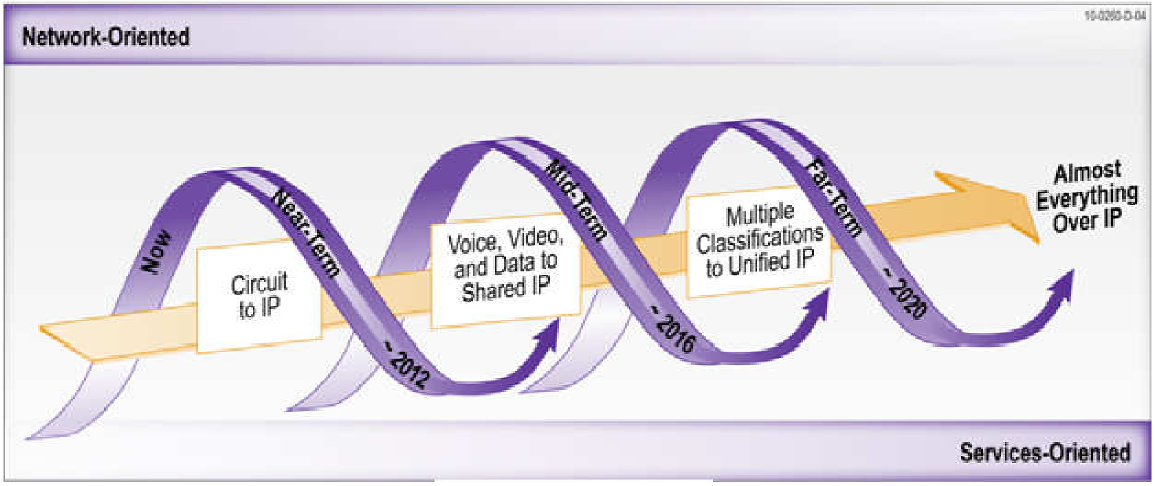


Figure 4.4-1. DISN Evolution Spirals

<u>Near-Term Spiral</u>. This Spiral focuses on enhancing the DISN IP data and transport services to transition from asynchronous transfer mode (ATM) and time division multiplexing (TDM) circuit-switched technologies to IP-based networks. Ethernet will become the standard interface for all DISN services. Converged voice, video, and data services will begin during this Spiral.

<u>Mid-Term Spiral</u>. This spiral will focus on expanding converged voice, video, and data services by integrating service specific networks into a shared IP-based network using improved IP QoS, multicast, and session setup technologies. Ethernet-based transport services will support different classification levels. Command and control applications will remain separate from the IP networks for mission assurance. High Assurance Internet Protocol Encryptor (HAIPE) deployments will be expanding. The phaseout of separate legacy circuit-based voice, video, and data networks in the DISN Mid-Term Spiral will expand as customers migrate to enhanced DISN

IP data services. Assured services will provide availability, information protection, and optimized information delivery.

Far-Term Spiral. This Spiral will focus on the DoD CIO’s vision for net-centricity by establishing highly available, resilient, and secure IP-based networks, to include command and control applications. This DISN spiral will support user-encrypted, IP-based voice, video, and data services at all classification levels over a unified customer interface.

4.4~~5~~ ~~VOICE AND VIDEO DESIGN FOR UNIFIED CAPABILITIES E2E NETWORKS DESCRIPTION~~NETWORK DESIGN FOR UC CAPABILITIES

This section provides a description of the E2E networks that use the UC products specified in Sections 5 and 6 that

- Establish the requirements needed by industry to develop requirements-compliant Unified Capability solutions,

- Provide the foundation for the development of Unified Capability Test Plans (UCTPs) for Interoperability and Information Assurance testing. These tests are used to make the certification decisions necessary to place products on the DoD UC APL.

- Provides Information Assurance requirements necessary for UC products to meet DoD Information Assurance policy to become approved products. Later, these Information Assurance requirements will be used to assist in the development of the STIGs needed to operate properly UC approved products once installed, and

- Identify only the MINIMUM requirements and features applicable to all DoD networks that support UC, which include voice and video operating in IP, converged networks with data services.

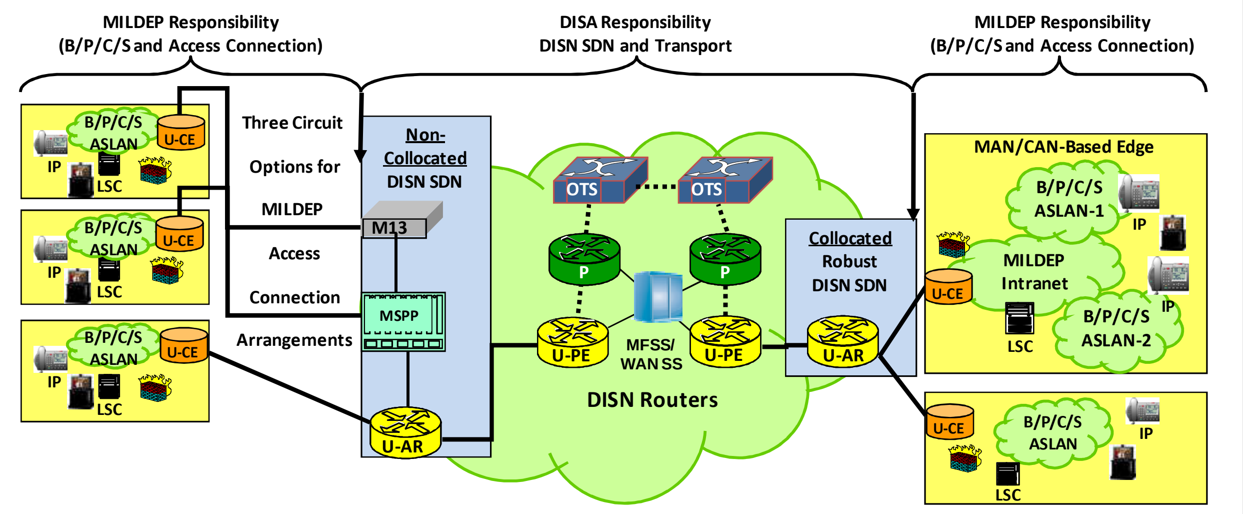
Sections 5 and 6 do not contain a complete set of requirements for the commercial off-the-shelf (COTS) features that do not affect assured services but are of interest to users, because these features do not provide interoperability with multiple vendors.

Specifically, this UCR specifies technical requirements for assured Interoperability and Information Assurance of products that provide the following set of UC, which will be expanded in the future:

- Voice and video services point-to-point

- Voice conferencing
- Videoconferencing
- E-mail/calendaring
- Unified messaging
- Web conferencing and web collaboration
- Unified conferencing
- Instant messaging and chat
- Rich presence
- Mobility

This section provides a network-level overview of the E2E network designs and the products that provide UC services. The E2E IP network design is illustrated in Figure 4.5-1, which shows the major components of the design and the responsibilities. The edge is made up of the UC-approved products, which include telephones, video codecs, assured services local area network (ASLANs), local session controllers (LSCs), Edge Boundary Controllers (EBCs), and the Customer Edge (CE) Routers. The edge is connected to the DISN SDNs and Transport via access circuits or via MILDEP Intranets.



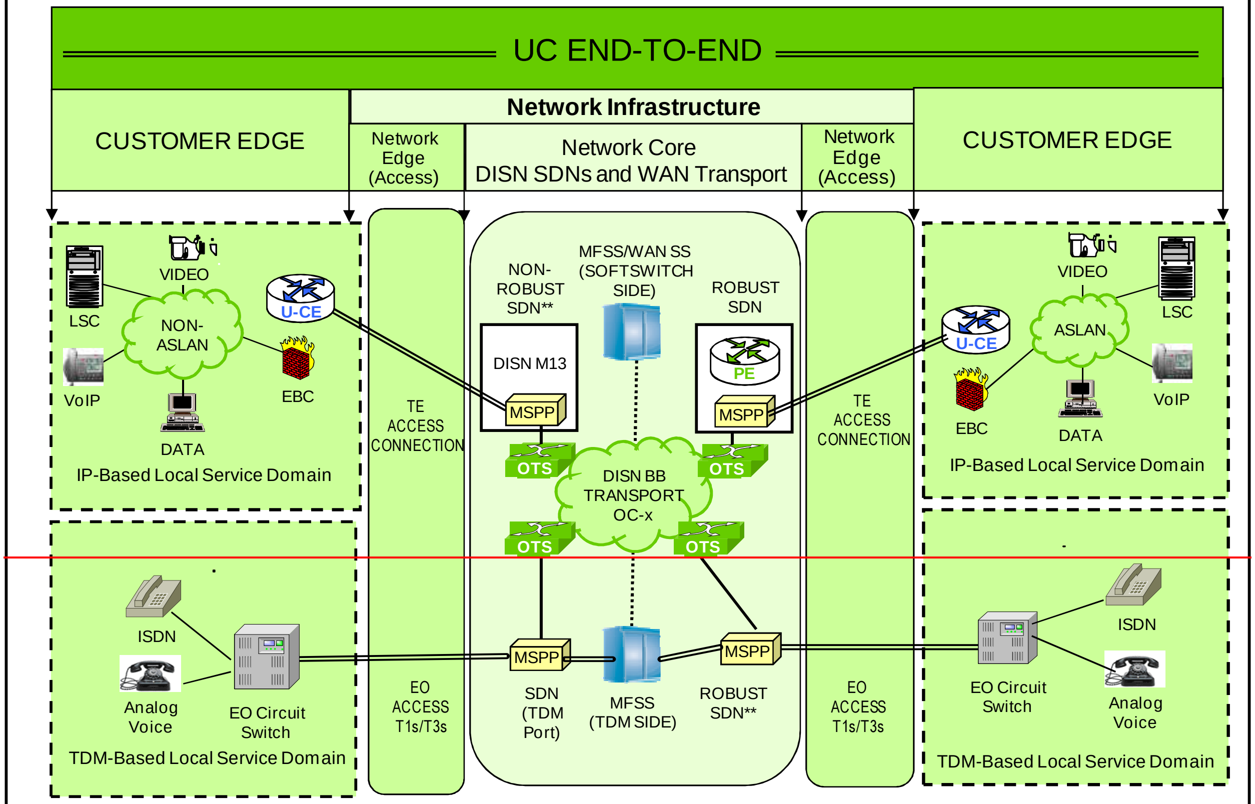
LEGEND

ASLAN	Assured Services Local Area Network	M13	Multiplexer	SDN	Service Delivery Node
B/P/C/S	Base, Post, Camp, Station	MAN	Metropolitan Area Network	SS	Softswitch
CAN	Campus Area Network	MFSS	Multifunction Softswitch	U-AR	Unclassified Aggregation Router
DISA	Defense Information Systems Agency	MILDEP	Military Department	U-CE	Unclassified Customer Edge Router
DISN	Defense Information System Network	MSPP	Multi-Service Provisioning Platform	U-PE	Unclassified Provider Edge Router
IP	Internet Protocol	OTS	Optical Transport System	WAN	Wide Area Network
LSC	Local Session Controller	P	Provider		

Figure 4.4~~5~~-1. E2E IP Network Description

Currently, the sensitive but unclassified (SBU) voice and integrated services digital network (ISDN) video services subset of UC are provided by the existing TDM-based defense Switched Network (DSN) and its components with Voice over Internet Protocol (VoIP) assured local area network (LAN) services provided to the telephone on ASLANs. The TDM-based services on the network backbone will migrate over a long period to IP-based assured services systems E2E, over the MILDEP ASLANs, Intranets, and the DISN network infrastructure. During the migration timeframe, SBU UC will be provided by a hybrid arrangement of both TDM- and IP-based systems. The Defense Red Switch Network (DRSN) will remain based on circuit-switched technologies as the only technologies that can currently provide multilevel security (MLS). However, classified VVoIP will migrate from the current Voice over Secure Internet Protocol (VoSIP) using the same network design as the SBU VVoIP with a few feature differences. In addition, the current DISN Video Services (DVS) VTC services will be provided predominately by DSN ISDN TDM technologies with a few sites capable of Video over IP for both SBU and classified VTCs. Eventually, SBU and classified VTC services will migrate to the SBU IP network design. Since the circuit-switched TDM-based network is well established, the following subsections provide a UC network overview by first describing VVoIP subsystems followed by an overview of the TDM-based DSN design.

Figure 4.4~~5~~-2 shows the three major E2E network segments: Customer Edge, Network Edge, and the Network Core (DISN SDNs and WAN Transport), which are all part of the UC E2E. End users attach to the Customer Edge Segment, consisting of either a TDM-based End Office (EO), or the set of VVoIP components of LSC, EBC, CE Router, and ASLAN. The Network Edge and the DISN Network Infrastructure are either TDM- or IP-based on the technology of the Edge. Within the DISN MFSS, the technology conversions necessary for the different technology edges to interoperate securely are performed.



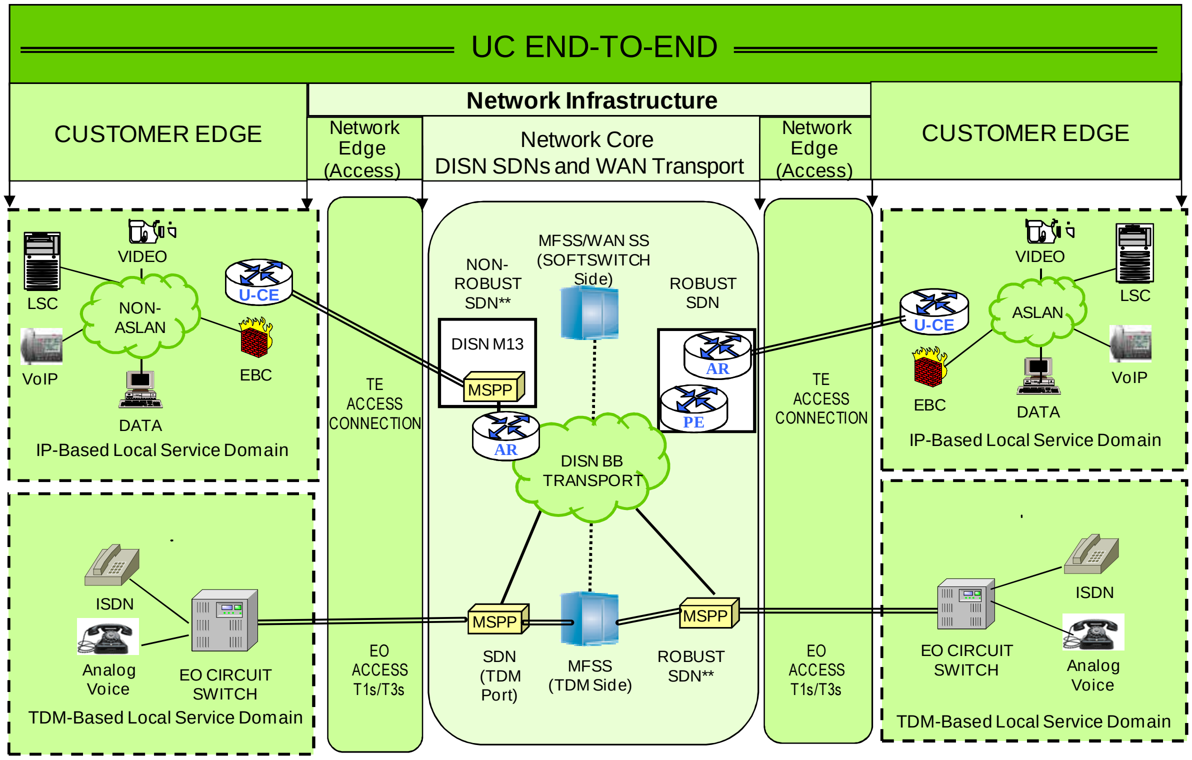
Simplified RTS Architecture Illustration: Sessions originate and terminate at local service domains within the GIG Edge Segments. End-to-End Service Interoperability among the TDM-based and IP-based RTS technology is achieved through the MFSS. The MFSS consists of a TDM side and a softswitch (IP) side.

*Two Types of LANs: Non-ASLAN and ASLAN

**Two Basic Types of SDNs: Robust and Non-Robust

LEGEND

ASLAN	Assured Services Local Area Network	LSC	Local Session Controller	RTS	Real Time Services
BB	Backbone	MFSS	Multifunction Softswitch	SDN	Service Delivery Node
B/P/C/S	Base, Post, Camp, Station	MSPP	Multi-Service Provisioning Platform	SS	Softswitch
C2	Command and Control	OC	Optical Carrier	TE	Traffic Engineering
CE	Customer Edge Router	OTS	Optical Transport System	U-CE	Unclassified Customer Edge Router
DISN	Defense Information System Network	P	Provider	VoIP	Voice over Internet Protocol
EBC	Edge Boundary Controller	PE	Provider Edge	WAN	Wide Area Network
GIG	Global Information Grid				



Simplified UC Architecture Illustration: Sessions originate and terminate at local service domains within the GIG Edge Segments.
End-to-End Service Interoperability among the TDM-based and IP-based UC technology is achieved through the MFSS.
The MFSS consists of a TDM side and a softswitch (IP) side.

LEGEND:

ASLAN	Assured Services LAN	GIG	Global Information Grid	P	Provider
BB	Backbone	LSC	Local Session Controller	PE	Provider Edge Router
B/P/C/S	Base/Post/Camp/Station	MFSS	Multifunction Softswitch	SDN	Service Delivery Node
C2	Command and Control	MSPP	Multi-Service Provisioning Platforms	TE	Traffic Engineered
CE	Customer Edge Router	OC	Optical Carrier	UC	Unified Capabilities
DISN	Defense Information Systems Network	OTS	Optical Transport System	U-CE	Unclassified CE Router
EBC	Edge Border Controller			VoIP	Voice over Internet Protocol
*Two Types of LANs: Non-ASLAN and ASLAN		** Two Basic Types of SDNs: Robust and Non-Robust		WAN	Wide Area Network

Figure 4.4~~5~~-2. High-Level Hybrid Voice and Video Network Design Illustrating the Three Main Network Segments

4.4~~5~~.1 Overview of Network Design ~~IP-Based Design~~ for ~~Unified Capabilities~~ VVoIP

This section provides a high-level overview of the VVoIP design within the context of the DoD network infrastructure. Because the details governing the complete VVoIP design and more specifically Assured Services are complex and consist of several components, individual sections are written within the UCR for each design component. The purpose of providing the high-level overview here is to give a consolidated view of the entire VVoIP as well as IM and Chat network infrastructures and services design.

There are two types of LANs: ASLAN and non-ASLAN. The mission of the subscriber (from both an origination and receiving role) determines which type of LAN to which they must attach.

The DISN consists of hundreds of worldwide SDNs interconnected by a highly robust, bandwidth-rich optical fiber cross-connected core with gigabit routers (i.e., the DISN Core). The customer is responsible for ensuring the aggregate access bandwidth on the Network Edge (Access) Segment is sized to meet the busy hour traffic demand for each service class and each of the four traffic queues, plus a 25 percent surge for voice and video traffic, plus a 10 percent aggregate overhead for signaling, NM, and routing traffic.

Based on a site's DISN Subscription Services (DSS) designation as a mission-critical site, the site's access to the DISN WAN may be dual homed. The major aspects determining the dual-homing method required, (i.e., the type of SDN that a user location shall connect to, the location of the Unclassified Customer Edge (U-CE) Router in relation to the type of SDN, and the type of missions that the U-CE Router serves), are as follows:

- Type of SDN
  - Non-Robust – M13 multiplexer
  - Robust –Multi-Service Provisioning Platform (MSPP) without Aggregation Router (AR) all with dual homing (assumes sufficient bandwidth with 50 percent over provisioning)
  - Robust – MSPP with Unclassified Aggregation Router (U-AR)
- U-CE Router Location for the SDN
  - U-CE Router not at an SDN location
  - U-CE Router at a non-robust SDN location
  - U-CE Router at a robust SDN location
- Type of U-CE Router
  - Critical mission
  - Noncritical mission

As shown in Figure 4.4~~5~~.1-1, a noncritical mission U-CE Router may connect to the nearest SDN regardless of the type of SDN, while a critical mission U-CE Router must be dual homed to two separate robust types of SDNs. If a critical mission U-CE Router is located on the same base as an SDN, it still requires a second connection to another robust SDN.

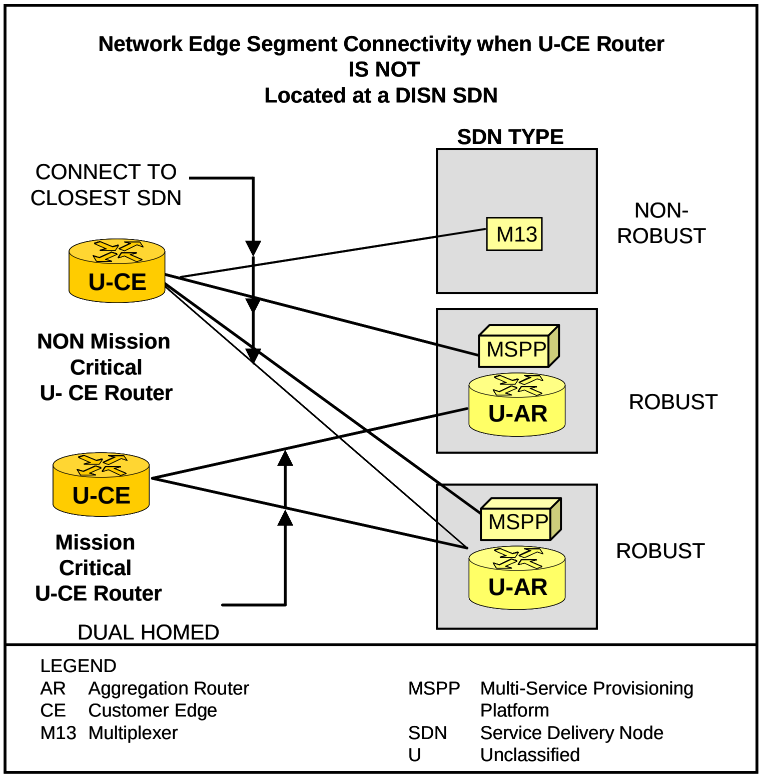
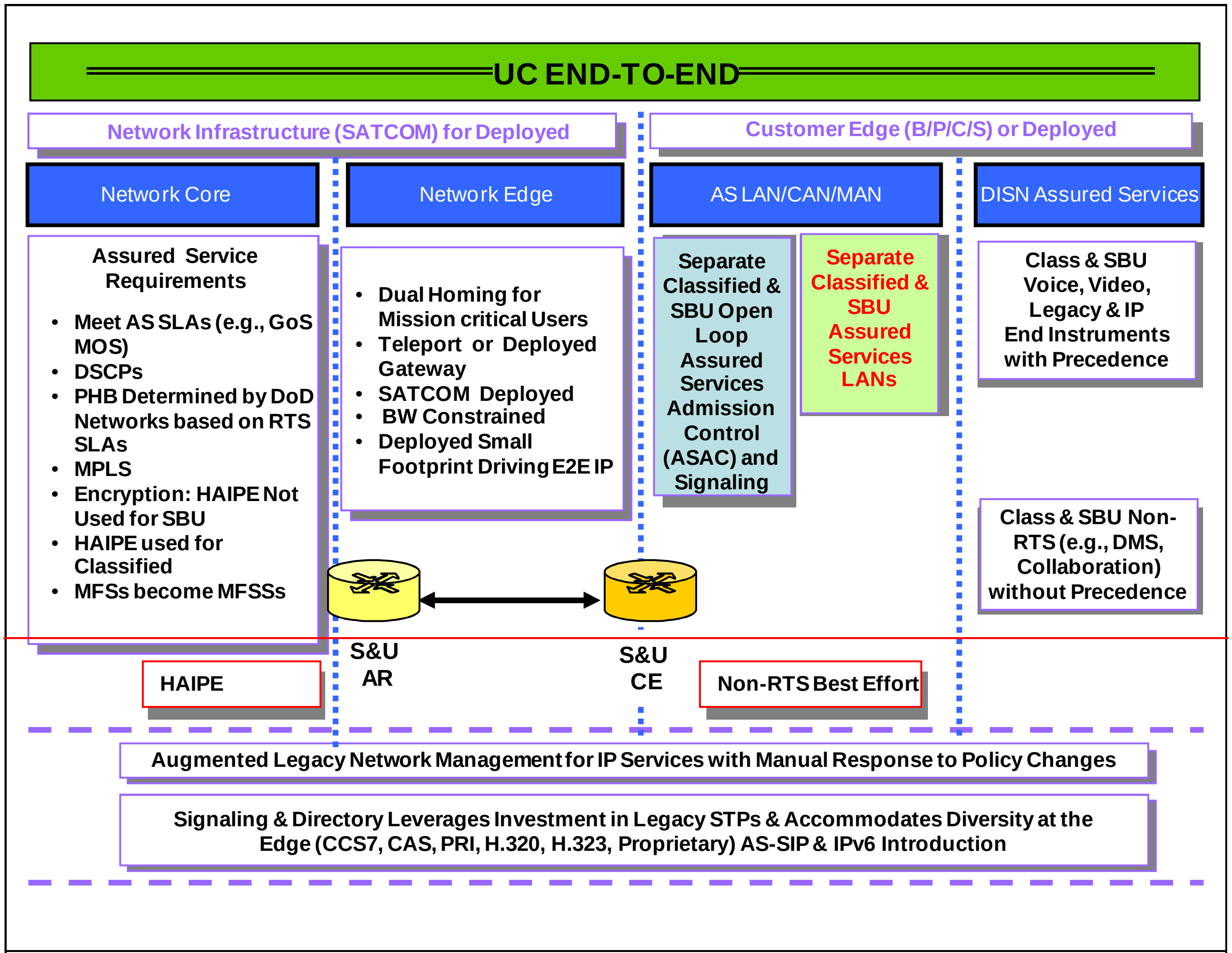


Figure 4.4~~5~~.1-1. Network Edge Segment Connectivity When U-CE Router is Not Located at SDN Site

4.4~~5~~.1.1 Overview of VVoIP Network Design Attributes

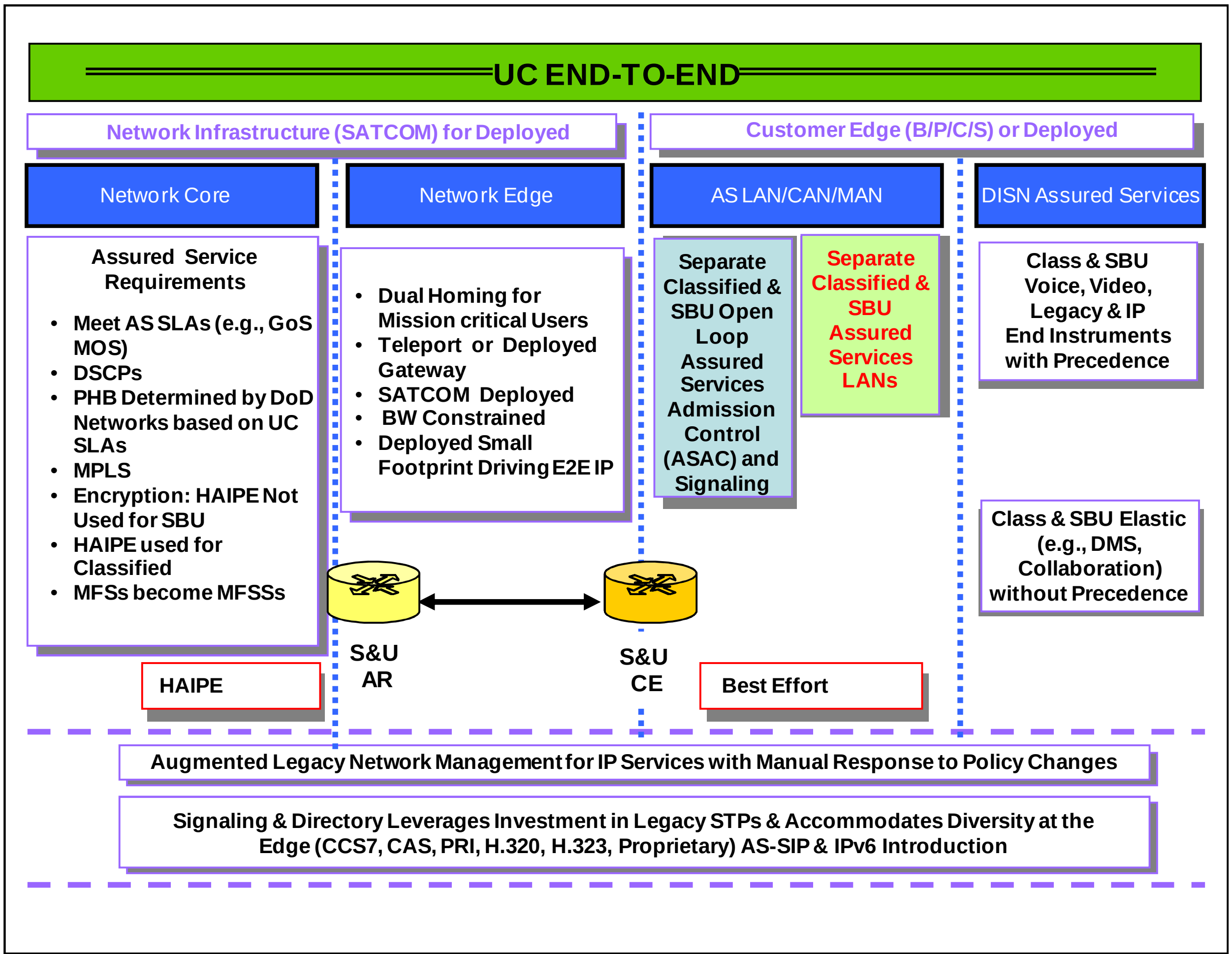
The most important consideration for implementing the VVoIP technology insertion associated with the “VVoIP Network Design” is not to degrade the capability to meet voice, video, and data services mission requirements. Preventing degradation begins with establishing a VVoIP Network Design and requirements that meet currently defined policies and requirements. The requirements will be validated and updated via both assessment testing in DoD laboratories and via the UC Spiral testing on operational networks as described in Section 4.4, Migration to Unified Capabilities.

The logical location of the major VVoIP network attributes within the UC E2E design is shown in Figure 4.4~~5~~.1-2, Overview of VVoIP network Attributes. The location of attributes in terms of the Customer Edge (B/P/C/S), the Network Edge (Access), and the Network Core is depicted, and the differentiation between assured service and non-assured service is shown between the top half of the diagram and the bottom half of the diagram, respectively.


UC END-TO-END
Network Infrastructure (SATCOM) for Deployed
Customer Edge (B/P/C/S) or Deployed
Network Core
Network Edge
AS LAN/CAN/MAN
DISN Assured Services
Assured Service Requirements
• Meet AS SLAs (e.g., GoS MOS)
• DSCPs
• PHB Determined by DoD Networks based on RTS SLAs
• MPLS
• Encryption: HAIPE Not Used for SBU
• HAIPE used for Classified
• MFSs become MFSSs
• Dual Homing for Mission critical Users
• Teleport or Deployed Gateway
• SATCOM Deployed
• BW Constrained
• Deployed Small Footprint Driving E2E IP
Separate Classified & SBU Open Loop Assured Services Admission Control (ASAC) and Signaling
Separate Classified & SBU Assured Services LANs
Class & SBU Voice, Video, Legacy & IP End Instruments with Precedence
Class & SBU Non-RTS (e.g., DMS, Collaboration) without Precedence
HAIPE
S&U AR
S&U CE
Non-RTS Best Effort
Augmented Legacy Network Management for IP Services with Manual Response to Policy Changes
Signaling & Directory Leverages Investment in Legacy STPs & Accommodates Diversity at the Edge (CCS7, CAS, PRI, H.320, H.323, Proprietary) AS-SIP & IPv6 Introduction

LEGEND:

AR	Aggregation Router	DSCP	Differentiated Services Code Point	MPLS	Multiprotocol Label Switching
AS	Assured Services	E2E	End to End		
ASAC	Assured Services Admission Control	GIG	Global Information Grid	OCONUS	Outside CONUS
AS-SIP	Assured Services SIP	GOS	Grade of Service	PHB	Per Hop Behavior
BW	Bandwidth	HAIPE	High Assurance Internet Protocol Encryptor	PRI	Primary Rate Interface
C2	Command and Control			RTS	Real Time Services
CAN	Campus Area Network	IP	Internet Protocol	S&U	Secret and Unclassified
CAS	Channel Associated Signaling	IPv6	Internet Protocol version 6	SATCOM	Satellite Communications
CCS7	Common Channel Signaling System No. 7	LAN	Local Area Network	SBU	Sensitive But Unclassified
		MAN	Metropolitan Area Network	SDN	Service Delivery Node
CE	Customer Edge Router	MFS	Multifunction Switch	SLA	Service Level Agreement
DISN	Defense Information Systems Network	MFSS	Multifunction Softswitch	STP	Signal Transfer Point
DMS	Defense Message System	MOS	Mean Opinion Score		


UC END-TO-END
Network Infrastructure (SATCOM) for Deployed
Customer Edge (B/P/C/S) or Deployed
Network Core
Network Edge
AS LAN/CAN/MAN
DISN Assured Services
Assured Service Requirements
Meet AS SLAs (e.g., GoS MOS)
DSCPs
PHB Determined by DoD Networks based on UC SLAs
MPLS
Encryption: HAIPE Not Used for SBU
HAIPE used for Classified
MFSs become MFSSs
Dual Homing for Mission critical Users
Teleport or Deployed Gateway
SATCOM Deployed
BW Constrained
Deployed Small Footprint Driving E2E IP
Separate Classified & SBU Open Loop Assured Services Admission Control (ASAC) and Signaling
Separate Classified & SBU Assured Services LANs
Class & SBU Voice, Video, Legacy & IP End Instruments with Precedence
Class & SBU Elastic (e.g., DMS, Collaboration) without Precedence
S&U AR
S&U CE
HAIPE
Best Effort
Augmented Legacy Network Management for IP Services with Manual Response to Policy Changes
Signaling & Directory Leverages Investment in Legacy STPs & Accommodates Diversity at the Edge (CCS7, CAS, PRI, H.320, H.323, Proprietary) AS-SIP & IPv6 Introduction

LEGEND:

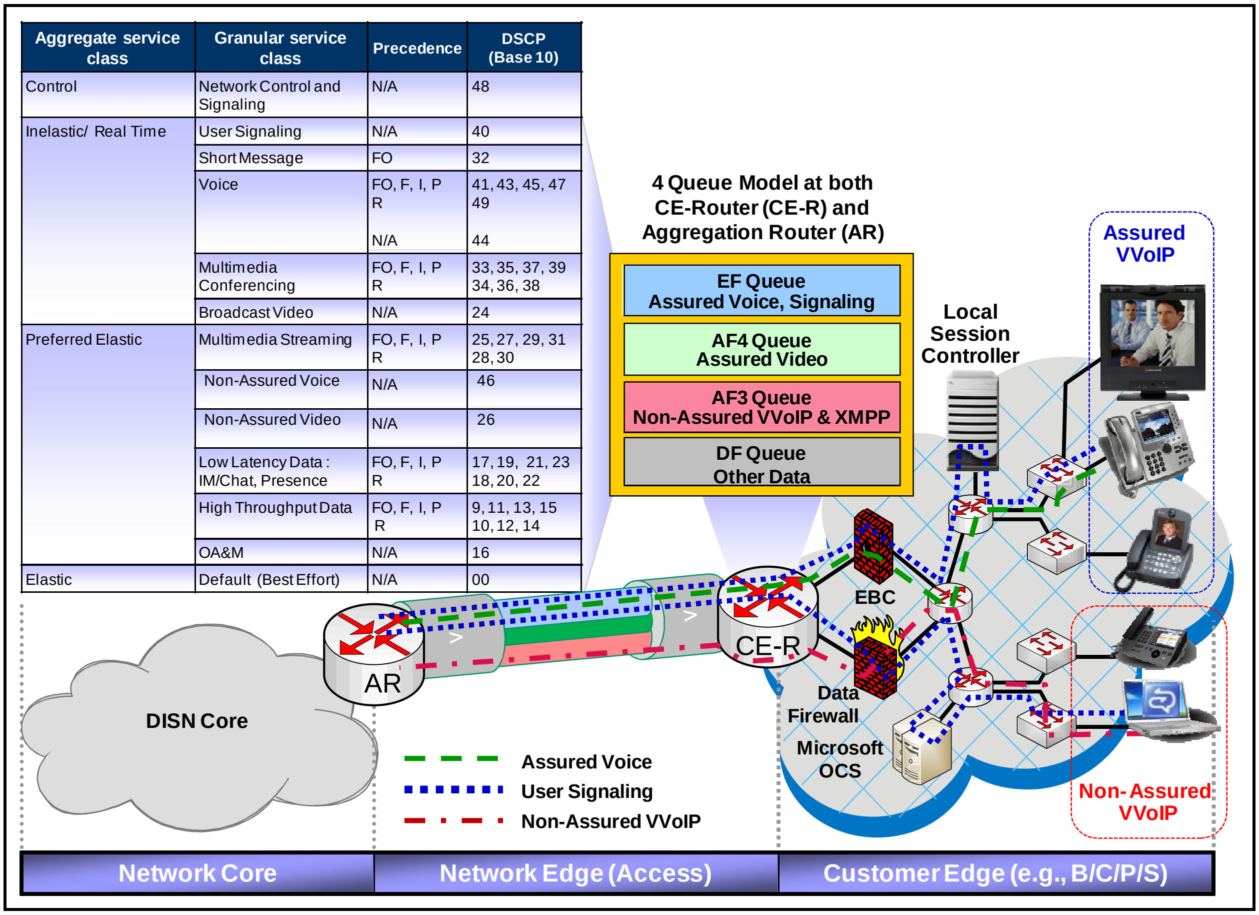
AR	Aggregation Router
AS	Assured Services
ASAC	Assured Services Admission Control
AS-SIP	Assured Services SIP
BW	Bandwidth
C2	Command and Control
CAN	Campus Area Network
CAS	Channel Associated Signaling
CCS7	Common Channel Signaling System No. 7
CE	Customer Edge Router
DISN	Defense Information Systems Network
DMS	Defense Message System
DSCP	Differentiated Services Code Point
E2E	End to End
GIG	Global Information Grid
GOS	Grade of Service
HAIPE	High Assurance Internet Protocol Encryptor
IP	Internet Protocol
IPv6	Internet Protocol version 6
LAN	Local Area Network
MAN	Metropolitan Area Network
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
OCONUS	Outside CONUS
PHB	Per Hop Behavior
PRI	Primary Rate Interface
S&U	Secret and Unclassified
SATCOM	Satellite Communications
SBU	Sensitive But Unclassified
SDN	Service Delivery Node
SLA	Service Level Agreement
STP	Signal Transfer Point

Figure 4.4~~5~~.1-2. Overview of VVoIP Network Attributes

The functions contained in the boxes located within the top half of Figure 4.4~~5~~.1-2 constitute the scope of the Assured Services functions while the placement of the boxes indicates where in the overall design (WAN to Edge) the functions logically reside. Voice, video, and data sessions are converged in the DISN WAN and the ASLAN, while currently only voice and video sessions are supported by Assured Services.

4.4~~5~~.1.1.1 Queuing Hierarchy for DISN IP Service Classes

Section 5.3.3, Network Infrastructure E2E Performance Requirements, defines a four-queue model for maintaining the required QoS for each UC Aggregate Service Class. Assured Voice, User Signaling, and Network Control Traffic are placed in the Expedited Forwarding (EF) queue. Assured Multimedia Conferencing (i.e., Video) traffic is placed in the Class 4 Assured Forwarding (AF4) queue. Preferred data, non-assured VVoIP; IM, Chat, and Presence; and Operations, Administration and Maintenance (OA&M) traffic is placed in the Class 3 Assured Forwarding (AF3) queue. All other traffic (data and any other service) are placed in the Best Effort (Default) queue. NOTE: User Signaling associated with non-assured VVoIP is placed in the EF queue. Figure 4.~~5~~4.1-3 shows the queue structure and associated rules.



Aggregate service class	Granular service class	Precedence	DSCP (Base 10)
Control	Network Control and Signaling	N/A	48
Inelastic/ Real Time	User Signaling	N/A	40
	Short Message	FO	32
	Voice	FO, F, I, P R N/A	41, 43, 45, 47 49 44
	Multimedia Conferencing	FO, F, I, P R	33, 35, 37, 39 34, 36, 38
	Broadcast Video	N/A	24
Preferred Elastic	Multimedia Streaming	FO, F, I, P R	25, 27, 29, 31 28, 30
	Non-Assured Voice	N/A	46
	Non-Assured Video	N/A	26
	Low Latency Data : IM/Chat, Presence	FO, F, I, P R	17, 19, 21, 23 18, 20, 22
	High Throughput Data	FO, F, I, P R	9, 11, 13, 15 10, 12, 14
	OA&M	N/A	16
Elastic	Default (Best Effort)	N/A	00

Figure 4.4~~5~~.1-3. Queuing for the Bearer Design

There are two categories of VVoIP. The first category is assured VVoIP and this category has been discussed in depth in earlier sections. The second category is non-assured VVoIP. Non-assured VVoIP has many of the same characteristics as assured VVoIP with two critical exceptions. The first exception is that session admission control (SAC) is not applied to non-assured VVoIP. SAC polices or controls the amount of sessions that are offered to the network. SAC can be provided by LSCs or Gatekeepers (i.e., H.323 Gatekeepers) and is associated with establishing a budget for the number of simultaneous sessions and ensuring that the number of active sessions is within that budget. ASAC extends SAC to allow sessions to be preempted when the SAC budget is at capacity and additional higher precedence sessions are offered. The second exception is that non-assured VVoIP sessions cannot be traffic engineered to ensure QoS. The ability to apply SAC to assured VVoIP ensures that assured VVoIP is deterministic or predictable in nature. Since the offered load is predictable it can be traffic engineered and the network can be designed for the traffic engineered load. Non-assured VVoIP does not have SAC and therefore cannot be traffic engineered to ensure that acceptable QoS is achieved. The nature of non-assured VVoIP is that it is typically composed of peer-to-peer sessions that do not transit a centralized SAC appliance and therefore SAC cannot be applied.

Mixing assured VVoIP with non-assured VVoIP will result in the uncontrolled non-assured VVoIP degrading assured VVoIP on congested networks. To ensure acceptable QoS in IP networks for assured VVoIP it is necessary to assign the assured VVoIP traffic to different queues than data sessions and non-assured VVoIP on congested connections. To delineate the assured VVoIP from the non-assured VVoIP (and other types of packets) it is necessary to mark the IP packets with unique DSCPs. Figure 4.4.1-3 provides a table of the DSCP plan and the queuing approach that is extracted from Section 5.3.3 of this document. In addition to queuing, it is also essential to apply traffic conditioning to the non-assured VVoIP packets since the packets are sent using the User Datagram Protocol (UDP) and are connectionless. This means that the host will continue transmitting at the same rate independent of the ability of the network to support that rate and the UDP packets can quickly cause the preferred data sessions that they are queued with (in four queue model) to terminate due to their use of Transmission Control Protocol (TCP), which responds to congestion by decreasing packet transmission rate. Enabling traffic conditioning on non-assured VVoIP packets will cause unacceptable degradation on non-assured VVoIP sessions during periods of high usage, but will ensure that preferred data sessions continue to get better than best effort performance in accordance with the UCR performance objectives.

The bandwidth for each queue must be provided based on a sound traffic engineering analysis, which includes the site budget settings, the site busy hour traffic load plus a 25 percent surge for voice and video traffic, plus a 10 percent aggregate overhead for signaling, NM, and routing traffic.

4.4~~5~~.1.1.2 Customer Edge Segment Design

The Customer Edge Segment has the following attributes:

1. **Nonblocking ASLAN**. At the Customer Edge, the design has an ASLAN that is designed as nonblocking for voice and video traffic.

2. **Traffic Admission Control**. The LSCs on a B/P/C/S use an Open Loop Assured Service Admission Control (ASAC) technique to ensure that only as many user-originated sessions (voice and video) in precedence order are permitted on the traffic-engineered access circuit consistent with maintaining a voice quality, as described in Section 5.3.3.15, Voice Service Quality.

3. **Call Preemption**. Lower precedence sessions will be preempted on the access circuit to accept the LSC setup of a higher precedence level outgoing or incoming session establishment request.

4. **Traffic Service Classification and Priority Queues**. In terms of the CE Router queuing structure, traffic will be assigned to the higher priority queues by an aggregated service class as described in UCR Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.

5. **MPLS and MPLS VPNs**. Can be implemented in the ASLAN but cannot be extended to the DISN.

RAE and Associated IT Infrastructure ~~–~~— See new Pp 4.4.1.1.2.5 Jo

4.4~~5~~.1.1.2.1 B/P/C/S VVoIP Design

The military B/P/C/S-level design consists of an LSC complex that may consist of a redundant LSC, or several LSCs in a cluster arrangement, in a LAN, campus area network (CAN), or metropolitan area network (MAN) structure. The LAN, CAN, or MAN design may be tailored to a single building or an entire base structure with varying degrees of robustness tailored to individual building mission requirements. Off-base connectivity to the long-haul DISN network infrastructure is provided through the EBC function. Interface to the local commercial telephone network is provided through a Media Gateway (MG) function within an LSC per local interface requirements. It is a MILDEP responsibility to design and fund the base infrastructure design.

4.5~~5~~.1.1.2.2 LSC Designs – Voice

An LSC is a call stateful voice, video, and signaling server product at the B/P/C/S that directly serves IP and analog EIs. The LSCs are the cornerstone of all DoD VVoIP signaling functions. The functions provided by the LSC are found in the MFSS also. The LSC may consist of one or more physical platforms. On the trunk side to the WAN, the LSC uses AS-SIP signaling. If the LSC interfaces to the public switched telephone network (PSTN) or to legacy B/P/C/S TDM systems, it must support Primary Rate Interface (PRI) also, using its MG and Media Gateway Controller (MGC). All LSCs provide PBAS via AS-SIP/ASAC for IP and via T1.619a.

Figure 4.4~~5~~.1-4, B/P/C/S-Level Voice over IP LSC Voice Designs, shows examples of three possible configurations for connecting multiple LSCs on a B/P/C/S to the DISN WAN and the MFSS. The U-CE Routers are dual homed and not shown for simplicity. At the top of the figure, the first case shown is where multiple LANs, each with its own LSC and U-CE Router, connect via separate access circuits to the DISN WAN. Each LSC would have its own traffic-engineered access circuit bandwidth, which can support the predetermined number of sessions (called a Budget in the figure). The limitation of this first case is that sessions from one LSC on the base to another LSC on the base must traverse the DISN WAN and use the MFSS to connect to another LSC. Should base connection to the DISN WAN or the MFSS be lost, then sessions from one base LSC to another on-base LSC could not be established. In addition, if one of the LSCs was not using all its traffic-engineered bandwidth (Budget A), a second LSC (Budget B) could not use the unused bandwidth of the other LSC (Budget A).

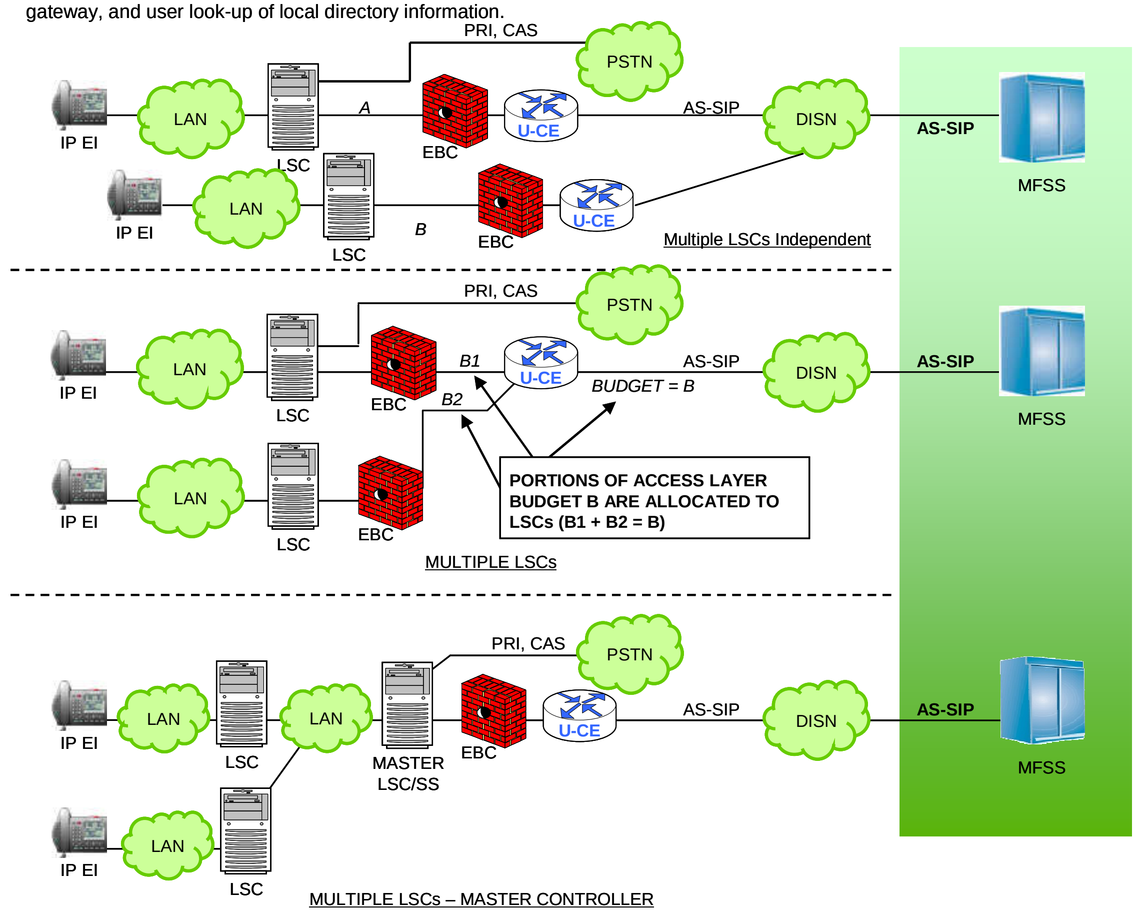
The second case, shown in the middle of the diagram, allows sessions to be established through the U-CE Router when connection to the DISN WAN is lost. Naturally, the access bandwidth connecting the common U-CE Router to the DISN WAN would need to be the sum of the traffic-engineered bandwidth for each individual LSC (i.e., $B = B_1 + B_2$). Again, if one LSC is not using all its budget/bandwidth, the other LSC cannot use the unused budget/bandwidth. For one LSC to establish a session to the other LSC, without access to the MFSS, then each LSC must contain the directory information of all LSCs on the base.

The third case, shown in the lower part of the figure, solves these limitations of being able to use all the WAN access circuit bandwidth, and the establishment of on-base sessions without the need for DISN WAN connection or access to an MFSS.

The third case requires the design and implementation of an LSC cluster concept where a master LSC, as shown in the figure, has a master directory of all users on the base. Under this arrangement, service order activity at one LSC will be reflected automatically at all LSCs in the cluster, including the master LSC. *Only the first case will be specified in detail in the UCR*. The other two cases will require custom engineering of the base design (including the use of the LSC portion of an MFSS where an MFSS is located on a base) to ensure interoperability and acceptable performance between the various on-base LSC arrangements and vendors.

BASE LEVEL ARCHITECTURES

LSCs must have “stand-alone” operational capabilities to serve the local domain (B/P/C/S) users in case the connection to the MFSS (or network-level softswitch) is severed. Required capabilities are in-domain (local) calling, routing of calls to/from PSTN gateway, and user look-up of local directory information.



LEGEND:

AS-SIP	Assured Services Session Initiation Protocol	EBC	Edge Boundary Controller	MFSS	Multifunction Softswitch
B/P/C/S	Base/Post/Camp/Station	EI	End Instrument	PRI	Primary Rate Interface
CAS	Channel Associated Signaling	IP	Internet Protocol	PSTN	Public Switched Telephone Network
CE	Customer Edge Router	LAN	Local Area Network	SS	Softswitch
DISN	Defense Information Systems Network	LSC	Local Session Controller	U	Unclassified

Figure 4.4~~5~~.1-4. B/P/C/S-Level Voice over IP LSC Designs

Some general rules to follow with respect to a master LSC and subtended LSCs are as follows:

1. End instruments served by a master LSC are treated like EIs served by subtended LSCs.

2. The master LSC adjudicates the enclave budget between the subtended LSCs.

3. Either of the following two methods is acceptable:

a. Method 1 – the master always ensures the highest priority sessions are served (up to the budget limit of the access link) regardless of the originating subtended LSC, for example,

(1) If the ASAC budget is 28.

(2) Each subtended LSC (3 total) allowed 10 voice sessions (10 budgets).

(3) Master LSC performs preemptions to ensure higher precedence sessions succeed.

(4) Master LSC blocks ROUTINE precedence sessions from any LSC after the access link budget is met.

b. Method 2 – the master maintains a strict budget for subtended LSCs, for example,

(1) If the ASAC budget is 30.

(2) Each subtended LSC (3 total) with each allowed 10 sessions.

(3) Does not use unfilled LSC budget to service above ROUTINE precedence sessions from another subtended LSC.

4. All LSCs directly connect to an EMS that supports the JTF-GNO.

5. The master LSC is not required to provide an aggregated NM view of the subtended LSCs.

6. Master LSCs and subtended LSCs communicate using AS-SIP and or proprietary signaling protocols if LSCs are from the same vendor.

a. All signaling destined external to the enclave passes through the master LSC.

b. Allows multiple vendors within the enclave or a single vendor integrated solution.

7. Each LSC maintains two budget counts as follows:

a. Intraenclave (based on local traffic engineering and not associated with the access link budget).

b. Interenclave (ASAC controlled by each LSC).

8. It is desired that connections to the PSTN only be through the master LSC (simplifies location services).

9. When a subtended LSC directly connects to the PSTN (exception situation, not desired), then only EIs of the subtended LSC can originate and receive calls from that PSTN PRI/CAS trunk.

10. The master LSC is the only connection to enclave TDM infrastructure (simplifies location services).

The choice of the B/P/C/S LSC configurations is dependent on the size of the B/P/C/S. Very small bases will have only one LSC so these configurations are not of concern. Larger B/P/C/Ss are most likely to have multiple circuit switches to replace, and might try to set up the LSC connections like their circuit switches, which would lead to the undesirable configurations that do not use master LSCs. Only the master configuration is recommended.

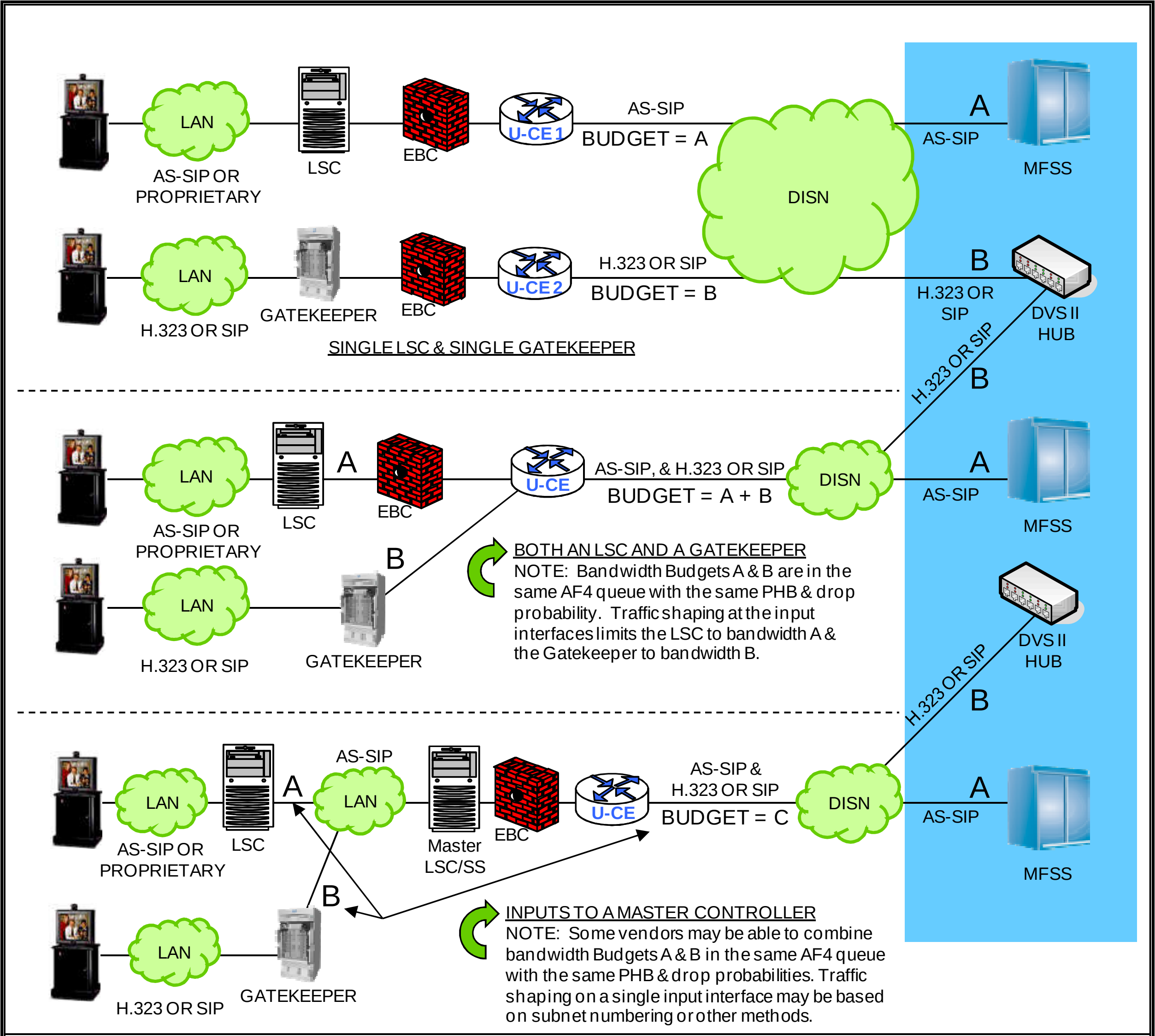
4.4~~5~~.1.1.2.3 LSC Designs – Video

Figure 4.4~~5~~.1-5, B/P/C/S Video over IP LSC Designs, illustrates the LSC designs for video services. An LSC is a call stateful AS-SIP signaling appliance at the B/P/C/S that directly serves IP video-capable EIs. The video LSC may consist of one or more physical platforms. On the trunk side to the WAN, the LSC uses AS-SIP signaling. A Gatekeeper is an appliance that processes calls to the WAN using H.323 or Session Initiation Protocol (SIP) signaling. If the LSC or Gatekeeper interfaces to the PSTN or to legacy B/P/C/S TDM appliances, it must also support PRI and channel-associated signaling (CAS) using its MG and MGC. All LSCs provide PBAS via AS-SIP/ASAC for IP and via MLPP for the PRI.

Figure 4.4~~5~~.1-5 shows examples of three possible configurations for connecting multiple video-capable LSCs and Gatekeepers on a B/P/C/S to the DISN WAN and the MFSS.

The first case is, shown at the top of the figure, where multiple LANs, one with its own LSC and U-CE Router, and another LAN with a Gatekeeper and U-CE Router that connect via separate access circuits to the DISN WAN. The LSC and the Gatekeeper would each have its own traffic-engineered access circuit bandwidth, which can support the predetermined number of sessions (called a Budget in the figure). The limitation of this first case is that sessions from the LSC or Gatekeeper on the base will not be able to communicate with each other because of the different signaling protocols in use by each. However, the LSC and the Gatekeeper each will have separate bandwidths that act independently to each other.

The second case, shown in the middle of the figure, allows sessions to be established through the U-CE Router. In this case, both the LSC and the Gatekeeper will act independently as described in the first case, but both will connect to the same U-CE Router. However, the LSC video call and the Gatekeeper video call will connect to separate ports on the U-CE Router. Naturally, the access bandwidth connecting the common U-CE Router to the DISN WAN would need to be the sum of the traffic-engineered bandwidth for each individual LSC (i.e., B1 + B2). Although each router port processing video calls acts independently in the AF4 queue, both customer calls must be treated equally when configured according to DoD policy.


LAN
AS-SIP OR PROPRIETARY
LSC
EBC
U-CE 1
AS-SIP
BUDGET = A
DISN
A
AS-SIP
MFSS
LAN
H.323 OR SIP
GATEKEEPER
EBC
U-CE 2
H.323 OR SIP
BUDGET = B
B
H.323 OR SIP
DVS II HUB
SINGLE LSC & SINGLE GATEKEEPER
H.323 OR SIP
B
LAN
AS-SIP OR PROPRIETARY
LSC
A
EBC
U-CE
AS-SIP, & H.323 OR SIP
BUDGET = A + B
DISN
A
AS-SIP
MFSS
LAN
H.323 OR SIP
GATEKEEPER
B
BOTH AN LSC AND A GATEKEEPER
NOTE: Bandwidth Budgets A & B are in the same AF4 queue with the same PHB & drop probability. Traffic shaping at the input interfaces limits the LSC to bandwidth A & the Gatekeeper to bandwidth B.
DVS II HUB
H.323 OR SIP
B
LAN
AS-SIP OR PROPRIETARY
LSC
A
AS-SIP
LAN
Master LSC/SS
EBC
U-CE
AS-SIP & H.323 OR SIP
BUDGET = C
DISN
A
AS-SIP
MFSS
B
LAN
H.323 OR SIP
GATEKEEPER
INPUTS TO A MASTER CONTROLLER
NOTE: Some vendors may be able to combine bandwidth Budgets A & B in the same AF4 queue with the same PHB & drop probabilities. Traffic shaping on a single input interface may be based on subnet numbering or other methods.

LEGEND:

AF	Assured Forwarding	DVS II	DISN Video Services II	MFSS	Multifunction Softswitch
AS-SIP	Assured Services Session Initiation Protocol	EBC	Edge Boundary Controller	PHB	Per Hop Behavior
CE	Customer Edge Router	LAN	Local Area Network	SIP	Session Initiation Protocol
DISN	Defense Information Systems Network	LSC	Local Session Controller	SS	Softswitch

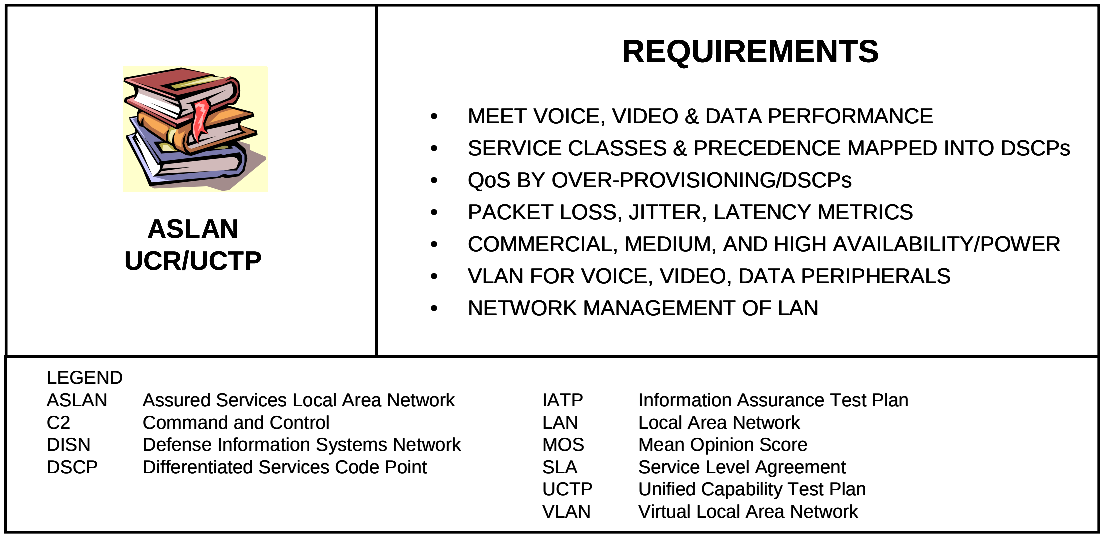
Figure 4.4~~5~~.1-5. B/P/C/S Video over IP LSC Designs

The third case requires the designation and implementation of an LSC cluster concept as described for the voice design in Section 4.4~~5~~.1.1.2.2, LSC Designs–Voice.

With regard to the Gatekeeper interworking with the master LSC or SS in the third case, some vendors may be able to manage the LSC-originated video call in addition to the Gatekeeper-originated call. In this case, the master LSC or SS will manage Budgets A and B to make a more efficient use of Budget C. Although the LSC video EI and the Gatekeeper EI will still not be able to communicate with each other because of different protocols utilized, the master LSC or SS will be able to process the calls into Budget C efficiently in the AF4 queue. All video calls leaving the master LSC or SS must be treated equally to comply with DoD policy.

4.4~~5~~.1.1.2.4 LAN and ASLAN Design

Requirements for the B/P/C/S LAN designs are defined in Section 5.3.1, Assured Services Local Area Network. The principal LAN requirements are summarized in Figure 4.4~~5~~.1-6.



REQUIREMENTS

- MEET VOICE, VIDEO & DATA PERFORMANCE
- SERVICE CLASSES & PRECEDENCE MAPPED INTO DSCPs
- QoS BY OVER-PROVISIONING/DSCPs
- PACKET LOSS, JITTER, LATENCY METRICS
- COMMERCIAL, MEDIUM, AND HIGH AVAILABILITY/POWER
- VLAN FOR VOICE, VIDEO, DATA PERIPHERALS
- NETWORK MANAGEMENT OF LAN

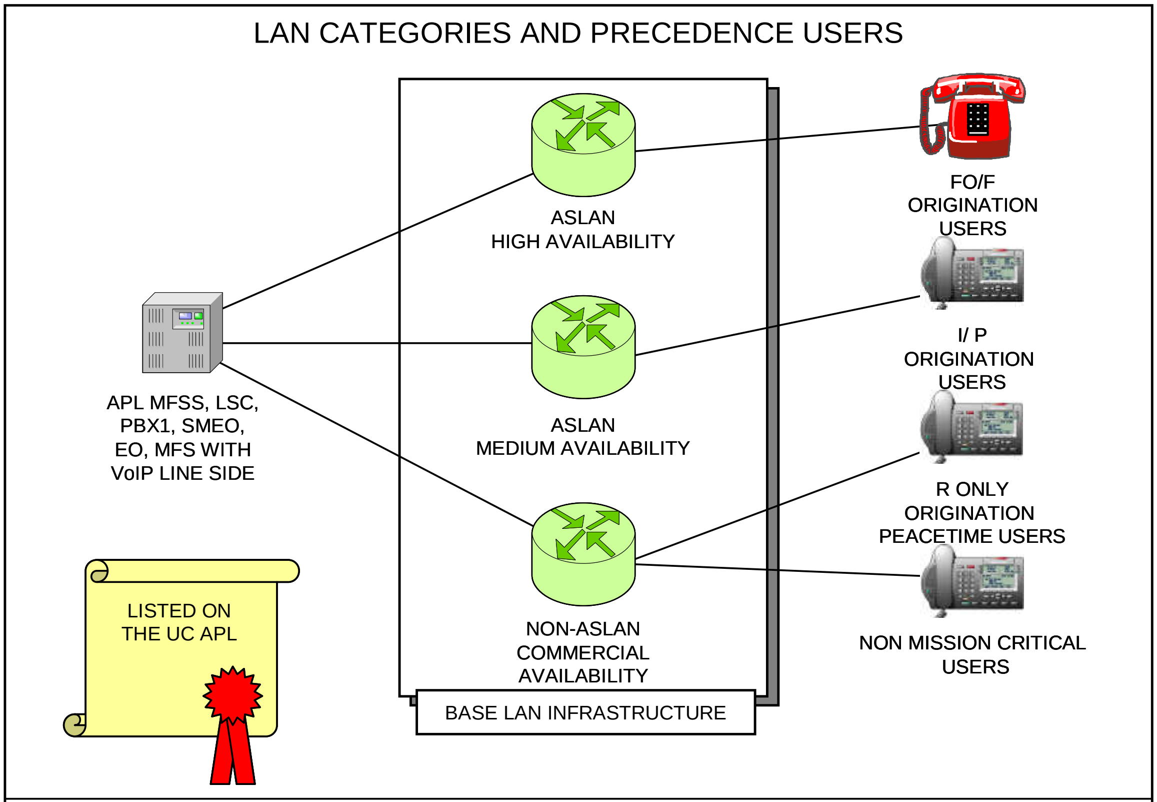
LEGEND

ASLAN	Assured Services Local Area Network	IATP	Information Assurance Test Plan
C2	Command and Control	LAN	Local Area Network
DISN	Defense Information Systems Network	MOS	Mean Opinion Score
DSCP	Differentiated Services Code Point	SLA	Service Level Agreement
		UCTP	Unified Capability Test Plan
		VLAN	Virtual Local Area Network

Figure 4.4~~5~~.1-6. ASLAN Requirements Summary

Two types of LANs are ASLAN and non-ASLAN, depending on the type of missions and users served by a LAN. The two LAN types and three categories along with user classes are illustrated in Figure 4.4~~5~~.1-7, Three Categories of LANs.

Table 4.4~~5~~.1-1, LAN Requirements Summary, shows the requirements needed based on subscriber mission category. *Requirements* are defined, as necessary, for the user while *Permitted* allows other user types to be served (such as a user that is authorized FLASH OVERRIDE and FLASH precedence is required to be served on a High Availability ASLAN, and other users are permitted on the same LAN). *Not Permitted* means that the user must not be served (such as a user that is authorized FLASH OVERRIDE and FLASH precedence cannot be served by a Medium Availability ASLAN or non-ASLAN). *Not Required* are requirements that do not have to be met for some users (such as requirements for diversity, redundancy, and power backup that are not required for users that only have ROUTINE precedence).



LEGEND		FO/F	Flash Override/Flash		
APL	Approved Products List	I/P	Immediate/Priority	P	Provider
ASLAN	Assured Services Local Area Network	LAN	Local Area Network	PBX1	Private Branch Exchange Type 1
EO	End Office	LSC	Local Session Contoller	R	Routine
JS	Joint Staff	MFS	Multifunction Switch	SMEO	Small End Office
		MFSS	Multifunction Softswitch	VoIP	Voice over Internet Protocol

Figure 4.4~~5~~.1-7. Three Categories of ASLANs

An ASLAN that supports users authorized I/P is classified as a Medium Availability ASLAN. An ASLAN that supports users authorized FO/F is classified as a High Availability ASLAN.

Table 4.4~~5~~.1-1. LAN Requirements Summary

LAN REQUIREMENT ITEM	USER PRECEDENCE ORIGINATION AUTHORIZATION			
	FO/F	I/P	R	NOT MISSION CRITICAL
ASLAN High	R	P	P	P
ASLAN Medium	NP	R	P	P
Non-ASLAN	NP	NP	P	P
ASF	R	R	R	N
Diversity	R	R	NR	NR
Redundancy	R	R	NR	NR
Battery Backup	8 hours	2 hours	NR	NR
Single Point of Failure User > 96 Allowed	No	No	Yes	Yes
GOS p=	0.0	0.0	0.0	Note 1
Availability	99.999	99.997	99.9	99.9

LEGEND

ASF	Assured Services Features	NP	Not Permitted
ASLAN	Assured Services LAN	NR	Not Required
FO/F	FLASH OVERRIDE/FLASH	P	Permitted
GOS	Grade of Service	R	Required
I/P	IMMEDIATE/PRIORITY	R	ROUTINE
LAN	Local Area Network		

Note 1 GOS is discretionary and shall be determined by DoD Components.

The actual LAN implementation will vary from base to base depending on building or facility locations, installed cable plant, and the location and type of missions being performed on the base. Figure 4.4~~5~~.1-8, An Example of a Potential CAN with a Mix of Mission and Non-Mission-Critical Users, is an example of one potential ASLAN implementation. It shows a CAN involving multiple buildings and types of mission users and how connectivity redundancy and backup power time requirement of 8, 2, or 0 hours are met in a cost-effective manner.

4.4.1.1.2.5 Regional ASLAN

Regional ASLAN designs are used where a local service enclave covers a large geographical area. Regional ASLANs typically consists of a single Security enclave, employ a distributed LSC architecture with redundancy and automatic failover of end instrument to a 'backup' LSC, high-speed links with MPLS at the LAN core layer, and Remote Media Gateways.

4.4.1.1.2.6 Required Ancillary Equipment

Operation of UC products requires support from server functions that normally are not part of an LSC or EBC product. These functions/severs are referred to as Required Ancillary Equipment (RAE) and must be made available at the site to support the LSC and EBC. RAE support includes authentication, Authorization and Accounting (AAA) servers, access to a Domain Name System (DNS) server, SYSLOG server, Network Time Protocol (NTP) server, Dynamic Host

Control Protocol (DHCP) server and, for PKI certificate verification, access to an Online Certificate Status Protocol (OCSP) responder.

4.4~~5~~.1.1.3 Network Infrastructure E2E Performance (DoD Intranets and DISN SDNs)

The DoD Intranets and the DISN SDNs serving SBU VVoIP traffic currently do not use HAIPEs. The DISN SDNs are assumed to be bandwidth-rich and robust. Since the ASLAN is required to be implemented as nonblocking for voice and video traffic, it has no bandwidth limit either. The access circuit, which can include a satellite communications (SATCOM) link from the Edge to the DISN Core SDN, is the only potential bandwidth-limited resource due to funding, crisis traffic surges, or damage. Therefore, the network design includes the use of ASAC to prevent session overload and subsequent voice and video performance degradation from the Customer Edge and to ensure that bandwidth is assigned to sessions based on precedence. The DISN WAN provides high availability (99.96 percent or greater) using dual-homed access circuits and the Multiprotocol Label Switching (MPLS) Fast Failure Recovery (FFR) in the Core.

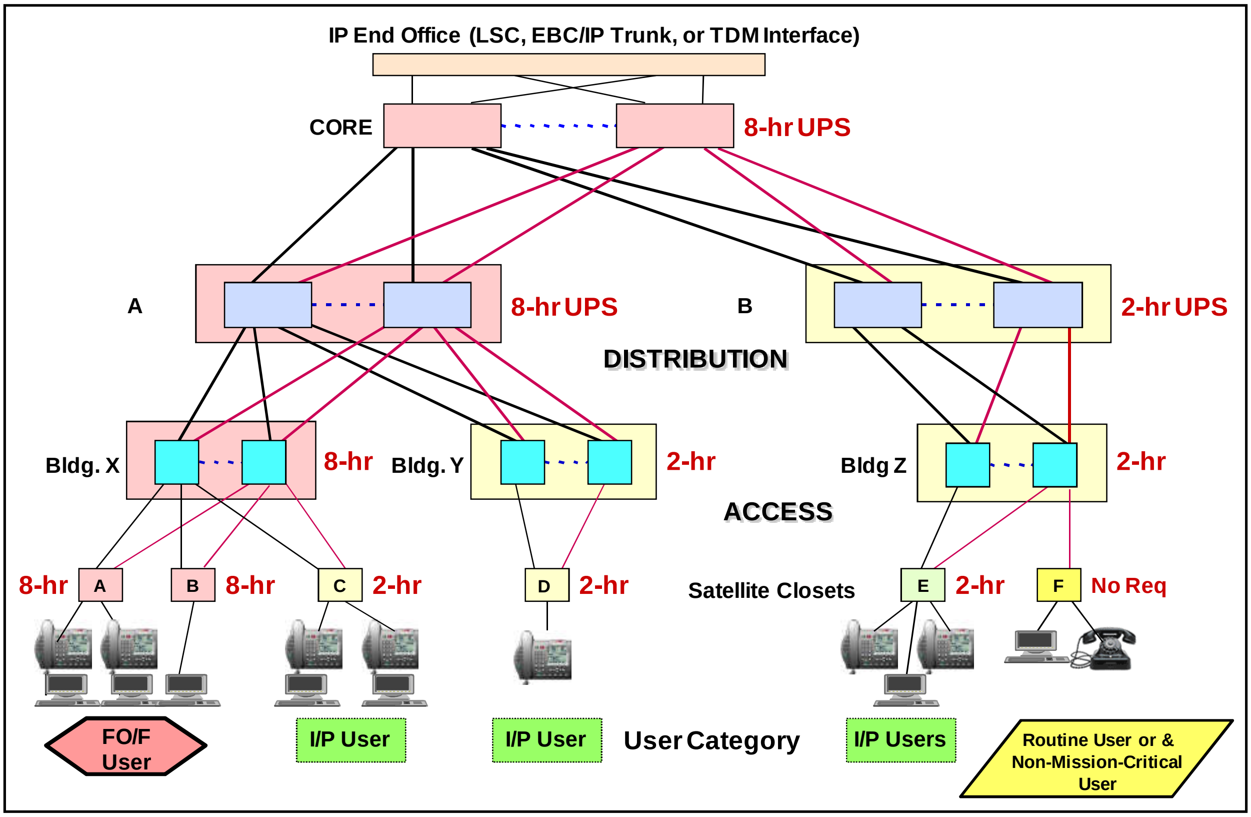
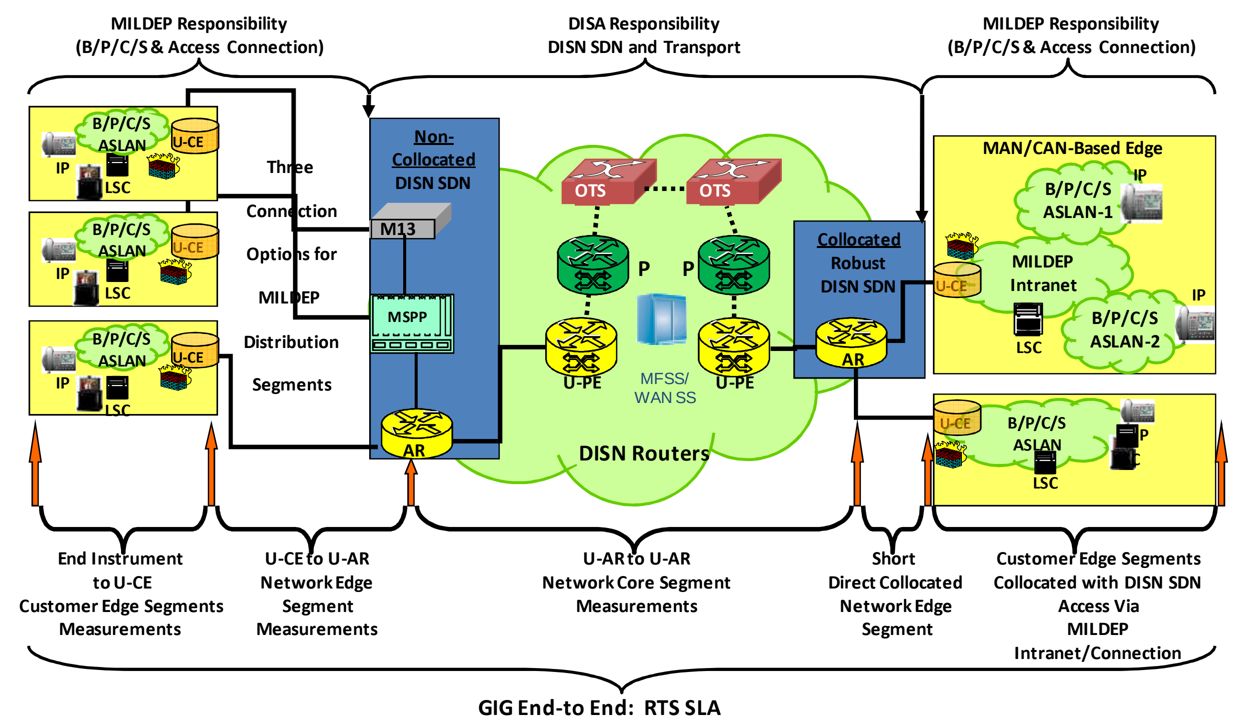


Figure 4.4~~5~~.1-8. An Example of a Potential CAN with a Mix of Mission and Non-Mission-Critical Users

In order to ensure E2E voice and video services' performance, an allocation of performance must be established for the Services' Intranets and DISN SDNs, which are supporting IP-based voice, video, and data services. The performance requirements for voice and video is based on best commercial practices for latency, packet loss, jitter, and availability, which is allocated to the Services' ASLANs and their associated CE Router and EIs, to the Services' Intranets (called MANs and CANs) and to the DISN SDNs. Many techniques, such as MPLS, Multiprotocol Label Switching – Traffic Engineered (MPLS-TE), queuing, mesh routing, and redundancy; can be used by the networks to meet the performance allocations. Currently, only the voice and video performance metrics have been defined. Data application performance metrics will be addressed in the future. The performance metrics for voice (E-Model R-Factor) and video have been defined. Measurement techniques for validating that the performance allocations have been met and for isolating the portion of the E2E network, that is not meeting the allocations have been developed. Figure 4.4~~5~~.1-9, Measurement Points for Network Segments, illustrates the components of the E2E network where measurements will be made to ascertain compliance with the Service Level Agreements (SLAs). The specific E2E network performance requirements are described in Section 5.3.3, Network Infrastructure E2E Performance Requirements.



Measurement Points ⬆ Illustrating End-to-End Allocation of Performance Parameters, by Network Segments. There are three Network Segments: the Customer Edge, Network Edge, and Core. The Customer Edge Segment is the infrastructure on the B/P/C/S that is the MILDEP 's responsibility. The Network Edge Segment is the Infrastructure between the B/P/C/S U-CE and DISN U-AR that is the MILDEP's responsibility to provision to the first DISA network component. For SLA measurement purposes, the U-AR is the measurement point for SLA budget allocation. The Network Core Segment is the infrastructure of the DISN SDNs and associated Transport that is the responsibility of DISA. The End-to-End Performance for Latency, Packet Loss, Jitter, and Availability is allocated and measured between the End Instruments and B/P/C/S U-CE, between the B/P/C/S U-CEs and the DISN U-ARs, and between the DISN U-ARs.

Figure 4.4~~5~~.1-9. Measurement Points for Network Segments

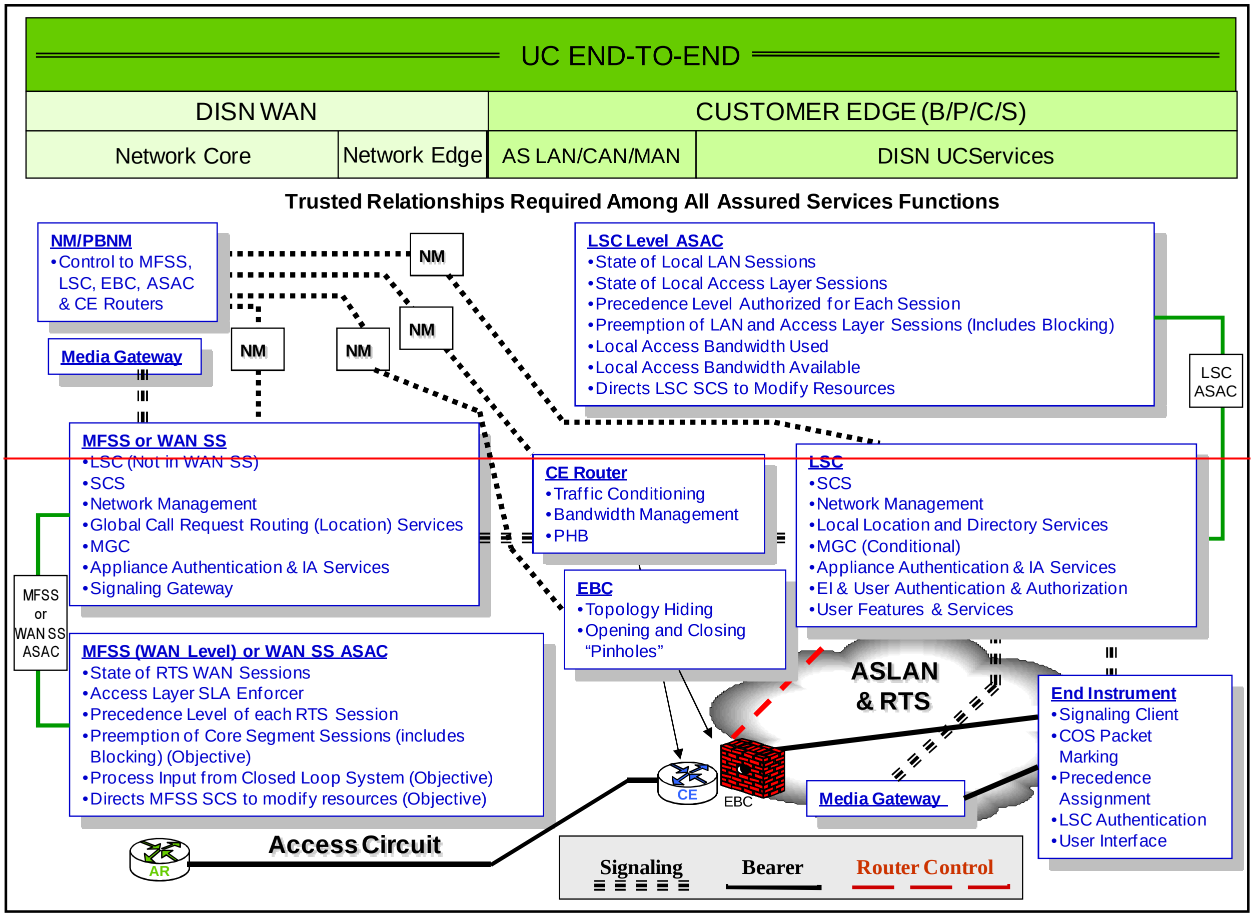
4.~~5~~4.1.1.4 E2E Protocol Planes

End-to-end services are set up, managed, and controlled by a series of functions and protocols that operate in three planes commonly referred to as signaling, bearer, and NM planes. The signaling plane is associated with the signaling and control protocols, such as AS-SIP, H.323, and Resource Reservation Protocol (RSVP). The bearer plane is associated with the bearer traffic and protocols, such as Secure Real-Time Transport Protocol (SRTP) and Real Time Control Protocol (RTCP). The NM plane is associated with NM protocols and is used to transfer status and configuration information between an NM system (NMS) and a network appliance. Network management protocols include the Simple Network Management Protocol (SNMP), Common Open Policy Service (COPS), and Secure Shell Version 2 (SSHv2).

4.~~5~~4.1.1.5 ASAC Component

The ASAC technique is the key VVoIP design component ensuring that E2E SLAs (Grade of Service (GOS) voice quality, user assured service delivery, and call preemption to the EI) are met in the converged DISN. The ASAC technique involves functional aspects of, and interactions among, virtually all network elements E2E.

Figure 4.4~~5~~.1-10 represents the first step in specifying the DISN ASFs by depicting a more detailed functional breakdown of the components than that shown in Figure 4.4~~5~~.1-2, Overview of VVoIP Network Attributes.


UC END-TO-END
DISN WAN
CUSTOMER EDGE (B/P/C/S)
Network Core
Network Edge
AS LAN/CAN/MAN
DISN UCServices
Trusted Relationships Required Among All Assured Services Functions
NM/PBNM
•Control to MFSS, LSC, EBC, ASAC & CE Routers
Media Gateway
NM
NM
NM
NM
LSC Level ASAC
•State of Local LAN Sessions
•State of Local Access Layer Sessions
•Precedence Level Authorized for Each Session
•Preemption of LAN and Access Layer Sessions (Includes Blocking)
•Local Access Bandwidth Used
•Local Access Bandwidth Available
•Directs LSC SCS to Modify Resources
LSC ASAC
MFSS or WAN SS
•LSC (Not in WAN SS)
•SCS
•Network Management
•Global Call Request Routing (Location) Services
•MGC
•Appliance Authentication & IA Services
•Signaling Gateway
CE Router
•Traffic Conditioning
•Bandwidth Management
•PHB
LSC
•SCS
•Network Management
•Local Location and Directory Services
•MGC (Conditional)
•Appliance Authentication & IA Services
•EI & User Authentication & Authorization
•User Features & Services
MFSS or WAN SS ASAC
EBC
•Topology Hiding
•Opening and Closing "Pinholes"
MFSS (WAN Level) or WAN SS ASAC
•State of RTS WAN Sessions
•Access Layer SLA Enforcer
•Precedence Level of each RTS Session
•Preemption of Core Segment Sessions (includes Blocking) (Objective)
•Process Input from Closed Loop System (Objective)
•Directs MFSS SCS to modify resources (Objective)
ASLAN & RTS
End Instrument
•Signaling Client
•COS Packet Marking
•Precedence Assignment
•LSC Authentication
•User Interface
CE
EBC
Media Gateway
AR
Access Circuit
Signaling
Bearer
Router Control

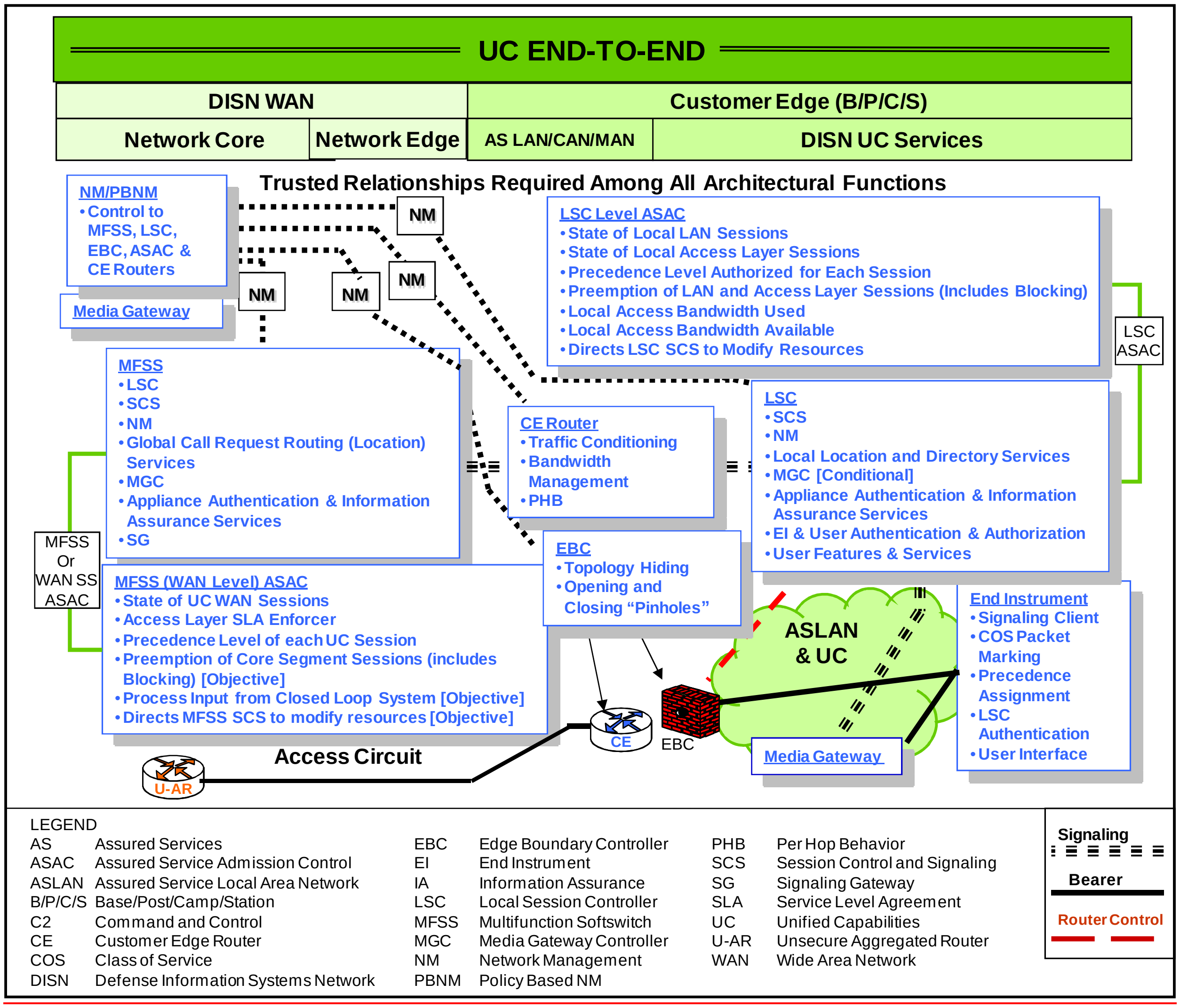

UC END-TO-END
DISN WAN
Customer Edge (B/P/C/S)
Network Core
Network Edge
AS LAN/CAN/MAN
DISN UC Services
Trusted Relationships Required Among All Architectural Functions
NM/PBNM
• Control to MFSS, LSC, EBC, ASAC & CE Routers
Media Gateway
NM
NM
NM
NM
LSC Level ASAC
• State of Local LAN Sessions
• State of Local Access Layer Sessions
• Precedence Level Authorized for Each Session
• Preemption of LAN and Access Layer Sessions (Includes Blocking)
• Local Access Bandwidth Used
• Local Access Bandwidth Available
• Directs LSC SCS to Modify Resources
LSC ASAC
MFSS
• LSC
• SCS
• NM
• Global Call Request Routing (Location) Services
• MGC
• Appliance Authentication & Information Assurance Services
• SG
CE Router
• Traffic Conditioning
• Bandwidth Management
• PHB
LSC
• SCS
• NM
• Local Location and Directory Services
• MGC [Conditional]
• Appliance Authentication & Information Assurance Services
• EI & User Authentication & Authorization
• User Features & Services
MFSS Or WAN SS ASAC
MFSS (WAN Level) ASAC
• State of UC WAN Sessions
• Access Layer SLA Enforcer
• Precedence Level of each UC Session
• Preemption of Core Segment Sessions (includes Blocking) [Objective]
• Process Input from Closed Loop System [Objective]
• Directs MFSS SCS to modify resources [Objective]
EBC
• Topology Hiding
• Opening and Closing "Pinholes"
ASLAN & UC
End Instrument
• Signaling Client
• COS Packet Marking
• Precedence Assignment
• LSC Authentication
• User Interface
Media Gateway
CE
EBC
Access Circuit
U-AR
LEGEND
AS Assured Services
ASAC Assured Service Admission Control
ASLAN Assured Service Local Area Network
B/P/C/S Base/Post/Camp/Station
C2 Command and Control
CE Customer Edge Router
COS Class of Service
DISN Defense Information Systems Network
EBC Edge Boundary Controller
EI End Instrument
IA Information Assurance
LSC Local Session Controller
MFSS Multifunction Softswitch
MGC Media Gateway Controller
NM Network Management
PBNM Policy Based NM
PHB Per Hop Behavior
SCS Session Control and Signaling
SG Signaling Gateway
SLA Service Level Agreement
UC Unified Capabilities
U-AR Unsecure Aggregated Router
WAN Wide Area Network
Signaling
Bearer
Router Control

Figure 4.4~~5~~.1-10. Assured Services Functions

Detailed requirements for each function contained in the boxes, the EBC, and the other components of the ASFs are contained in Section 5.3.2, Assured Services Features Requirements.

The Open Loop ASAC design, depicted in Figure 4.4~~5~~.1-11, Open Loop ASAC Network Design, is specified as the current method for achieving assured services E2E. The ASLAN connects via a local access circuit to a backbone network that consists of a Core MPLS-capable network.

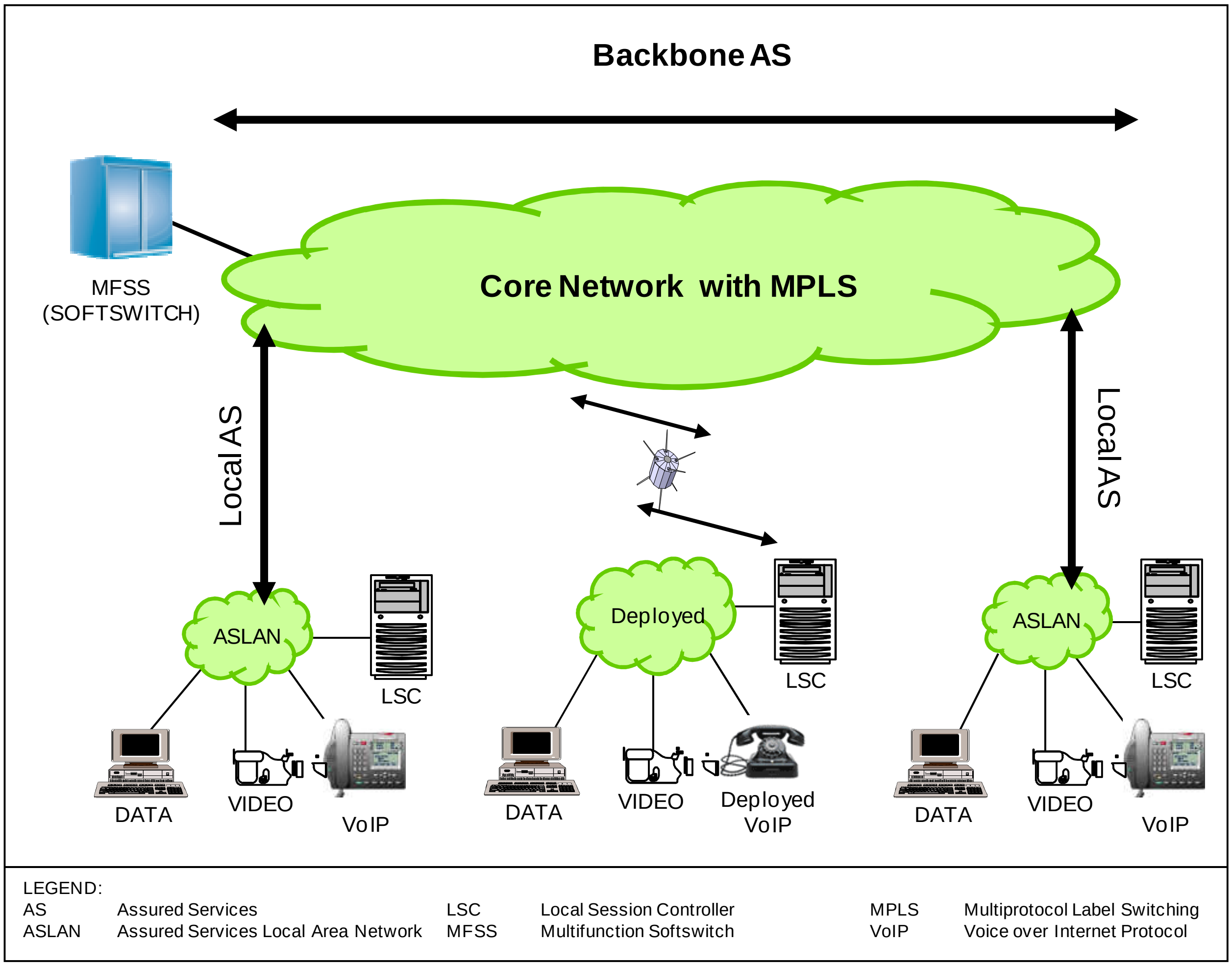
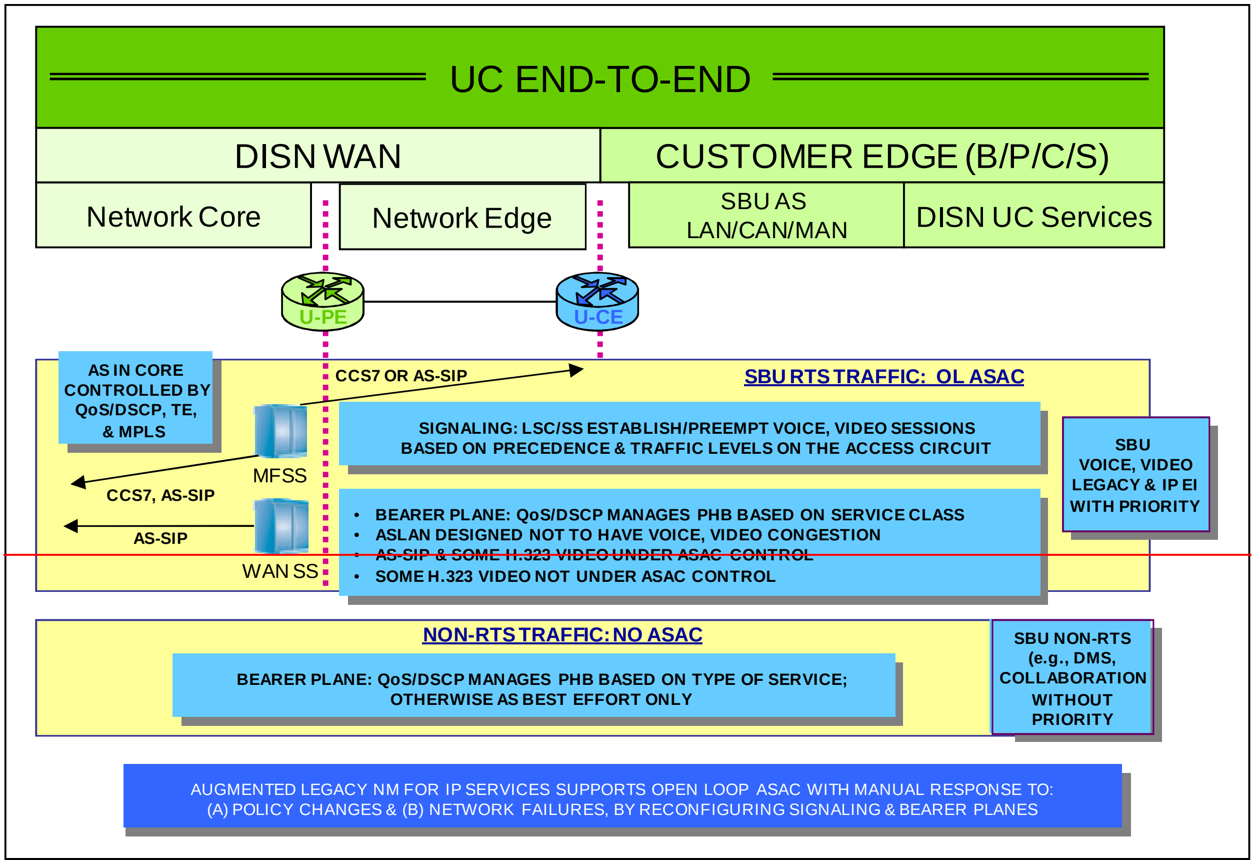

Backbone AS
MFSS
(SOFTSWITCH)
Core Network with MPLS
Local AS
Local AS
ASLAN
LSC
Deployed
LSC
ASLAN
LSC
DATA
VIDEO
VoIP
DATA
VIDEO
Deployed
VoIP
DATA
VIDEO
VoIP
LEGEND:
AS Assured Services
ASLAN Assured Services Local Area Network
LSC Local Session Controller
MFSS Multifunction Softswitch
MPLS Multiprotocol Label Switching
VoIP Voice over Internet Protocol

Figure 4.4~~5~~.1-11. Open Loop ASAC Network Design

The local assured services domain consists of an EI, ASLAN, LSC, and access circuit. Both the local assured services domains and the backbone assured services domains are realized with functionality in the signaling plane and the bearer plane to initiate and sustain a voice and video session.

NOTE: Deployable VoIP products may connect via compressed satellite circuits to the DISN backbone and operate in a similar manner to fixed products on an ASLAN.

The components of the Open Loop ASAC method are shown in Figure 4.4~~5~~.1-12, Open Loop ASAC for SBU Voice and Video. In the access circuit and the ASLAN, AS-SIP signaling (see Section 5.3.4, AS-SIP General Specification) is used by the LSC and MFSS to establish or preempt voice and video sessions based on precedence and engineered traffic levels on the access circuits (both origination and destination ends). In the bearer plane, the QoS/DSCP manages router per-hop behavior (PHB) based on the type of service class. Both the ASLAN and the backbone are assumed to be traffic engineered to be nonblocking for voice and video traffic. In the DISN Core, the DISN SLAs will support voice and video with assured services provided by QoS/Differentiated Service Code Point (DSCP), traffic engineering, and MPLS. Traffic with no marking will be treated as Best Effort.



SIGNALING: LSC/SS ESTABLISH/PREEMPT VOICE, VIDEO SESSIONS BASED ON PRECEDENCE & TRAFFIC LEVELS ON THE ACCESS CIRCUIT

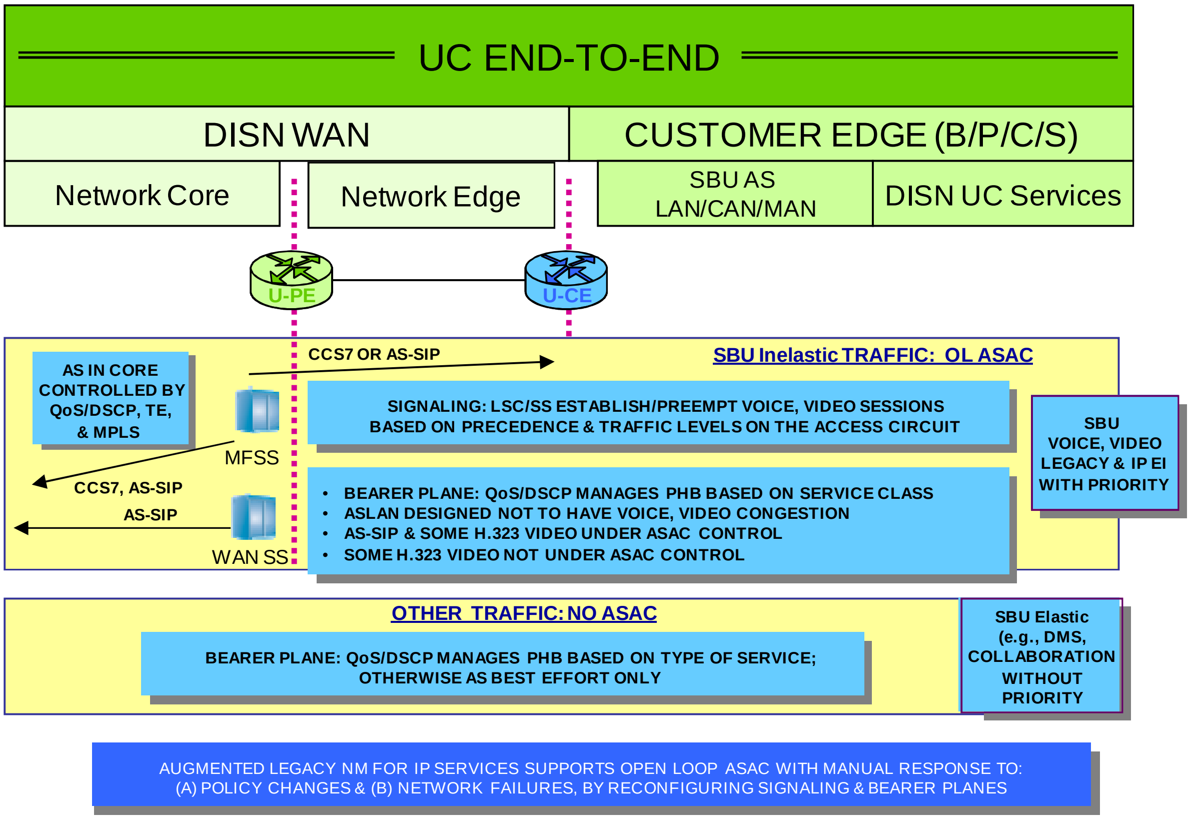
- BEARER PLANE: QoS/DSCP MANAGES PHB BASED ON SERVICE CLASS
- ASLAN DESIGNED NOT TO HAVE VOICE, VIDEO CONGESTION
- ~~AS-SIP & SOME H.323 VIDEO UNDER ASAC CONTROL~~
- SOME H.323 VIDEO NOT UNDER ASAC CONTROL

BEARER PLANE: QoS/DSCP MANAGES PHB BASED ON TYPE OF SERVICE; OTHERWISE AS BEST EFFORT ONLY

AUGMENTED LEGACY NM FOR IP SERVICES SUPPORTS OPEN LOOP ASAC WITH MANUAL RESPONSE TO: (A) POLICY CHANGES & (B) NETWORK FAILURES, BY RECONFIGURING SIGNALING & BEARER PLANES

LEGEND

AS	Assured Services	EI	End Instrument	QoS	Quality of Service
ASAC	Assured Service Admission Control	LAN	Local Area Network	RTS	Real Time Services
AS-SIP	Assured Services Session Initiation Protocol	LSC	Local Session Controller	SBU	Sensitive but Unclassified
B/P/C/S	Base/Post/Camp/Station	MAN	Metropolitan Area Network	SS	Softswitch
C2	Command and Control	MFSS	Multifunction Softswitch	TE	Traffic Engineered
CAN	Campus Area Network	MPLS	Multiprotocol Label Switching	UC	Unified Capabilities
CCS7	Common Channel Signaling System No. 7	NM	Network Management	U-CE	Unclassified Customer Edge
DISN	Defense Information Systems Network	OL	Open Loop	U-PE	Unclassified Provider Edge
DMS	Defense Message System	PHB	Per-Hop Behavior	WAN	Wide Area Network
DSCP	Differentiated Services Code Point				


UC END-TO-END
DISN WAN
CUSTOMER EDGE (B/P/C/S)
Network Core
Network Edge
SBU AS LAN/CAN/MAN
DISN UC Services
U-PE
U-CE
CCS7 OR AS-SIP
SBU Inelastic TRAFFIC: OL ASAC
AS IN CORE CONTROLLED BY QoS/DSCP, TE, & MPLS
MFSS
SIGNALING: LSC/SS ESTABLISH/PREEMPT VOICE, VIDEO SESSIONS BASED ON PRECEDENCE & TRAFFIC LEVELS ON THE ACCESS CIRCUIT
SBU VOICE, VIDEO LEGACY & IP EI WITH PRIORITY
CCS7, AS-SIP
AS-SIP
WAN SS
BEARER PLANE: QoS/DSCP MANAGES PHB BASED ON SERVICE CLASS
ASLAN DESIGNED NOT TO HAVE VOICE, VIDEO CONGESTION
AS-SIP & SOME H.323 VIDEO UNDER ASAC CONTROL
SOME H.323 VIDEO NOT UNDER ASAC CONTROL
OTHER TRAFFIC: NO ASAC
BEARER PLANE: QoS/DSCP MANAGES PHB BASED ON TYPE OF SERVICE; OTHERWISE AS BEST EFFORT ONLY
SBU Elastic (e.g., DMS, COLLABORATION WITHOUT PRIORITY
AUGMENTED LEGACY NM FOR IP SERVICES SUPPORTS OPEN LOOP ASAC WITH MANUAL RESPONSE TO: (A) POLICY CHANGES & (B) NETWORK FAILURES, BY RECONFIGURING SIGNALING & BEARER PLANES

LEGEND:

AS	Assured Services	EI	End Instrument	PHB	Per-Hop Behavior
ASAC	Assured Service Admission Control	GIG	Global Information Grid	QoS	Quality of Service
AS-SIP	Assured Services Session Initiation Protocol	LAN	Local Area Network	SBU	Sensitive but Unclassified
B/P/C/S	Base/Post/Camp/Station	LSC	Local Session Controller	SS	Softswitch
C2	Command and Control	MAN	Metropolitan Area Network	TE	Traffic Engineered
CAN	Campus Area Network	MFSS	Multifunction Softswitch	U-CE	Unclassified Customer Edge
CCS7	Common Channel Signaling System No. 7	MPLS	Multiprotocol Label Switching	U-PE	Unclassified Provider Edge
DISN	Defense Information Systems Network	NM	Network Management	WAN	Wide Area Network
DMS	Defense Message System	OL	Open Loop		
DSCP	Differentiated Services Code Point				

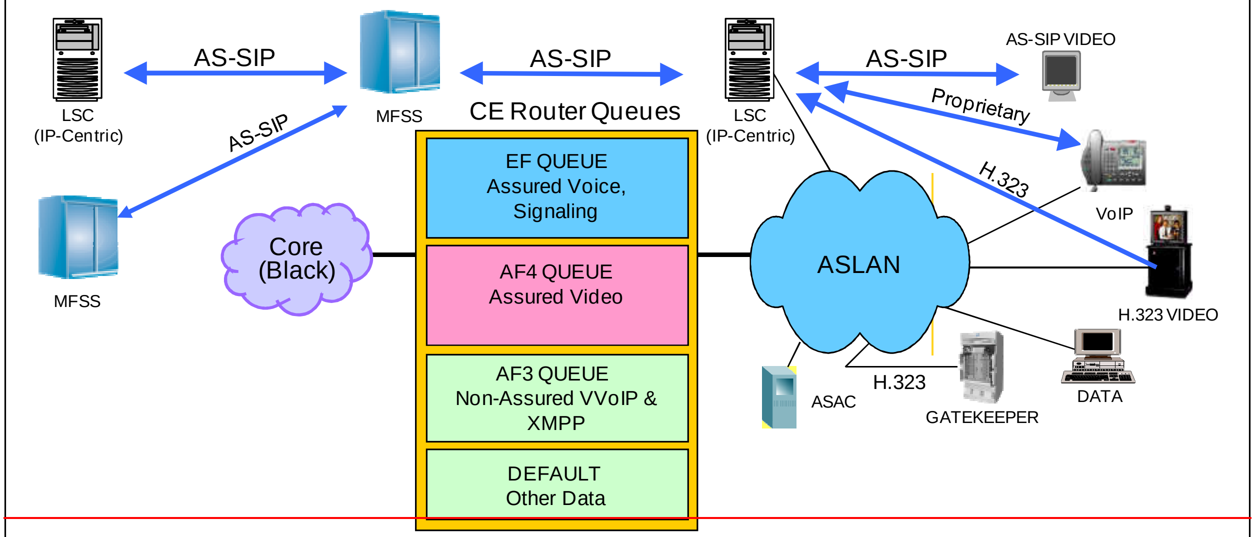
Figure 4.4~~5~~.1-12. Open Loop ASAC for SBU Voice and Video

The LSC manages a budget for sessions determined by the voice and video traffic-engineered bandwidth of the associated access infrastructure. The Resource-Priority header portion of the AS-SIP signaling message conveys the precedence of the desired session establishment to the destination end LSC. Both the originating and destination LSCs independently manage their session budgets, so that sessions are permitted or established by precedence until the budget limit is reached. Then a new session can be allowed only if a lower precedence session is available to preempt. At the originating end after preemption has taken place, if necessary, the origination request is sent to the destination upon which, after preemption has taken place, if necessary, the request acceptance is returned to the originating LSC. If the originating LSC is at its budget limit and has no lower precedence session to preempt, then a blocked session indication, in the form of a Blocked Precedence Announcement (BPA), will be sent to the originating EI. If the terminating LSC is at its budget limit and has no lower precedence session to preempt, then a

Session Request Denied message will be returned to the originating LSC, which, in turn, will send a BPA to the EI. For ROUTINE precedence calls reaching the maximum budget limit, “fast busy” (120 impulses per minute (ipm)) will be sent to the originating EI. All AS-SIP voice users and some H.323 video users will come under Open Loop ASAC. Some H.323 video users on a base may choose to use a separate H.323 Gatekeeper and not come under LSC Open Loop ASAC.

NOTE: Data traffic (non-voice and video) does not have any ASAC and is handled as Best Effort or preferred data, if the data application implements DSCP packet marking. Figure 4.4~~5~~.1-13, Converged VVoIP Design: Signaling, QoS, and Assured Service, shows the aspects of ASAC, signaling, and QoS (CE Router queues and PHB) in one diagram.

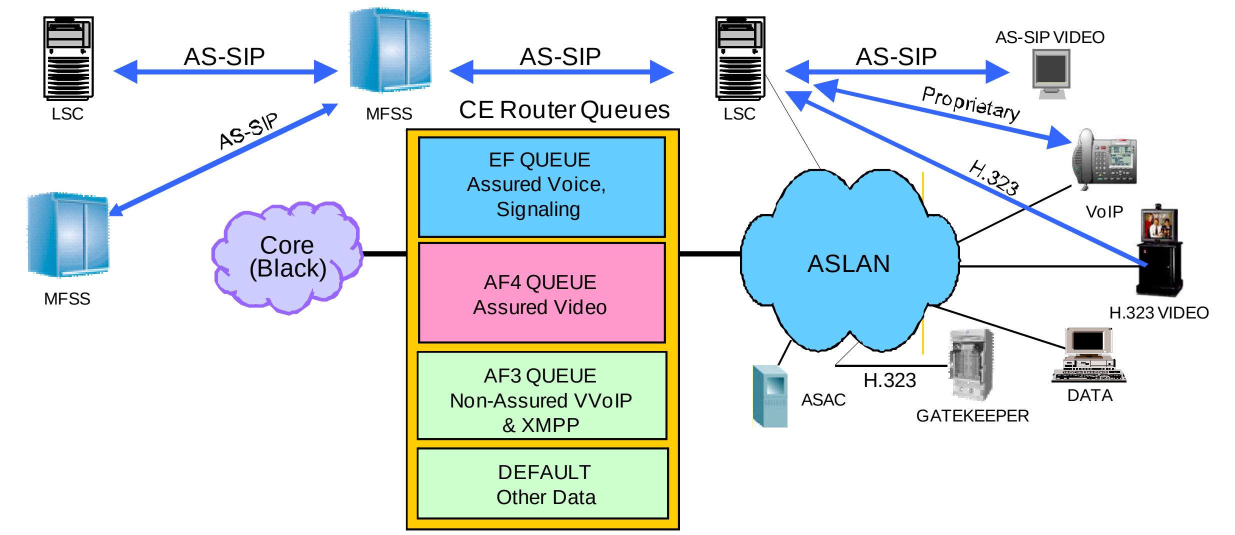
Session control processing to establish, maintain, and terminate sessions is performed by the Call Connection Agent (CCA) part of the LSC and MFSS. Signaling is performed by the Signaling Gateway (SG) (used for CCS7), the MG (for CAS), or the AS-SIP signaling appliance part of the LSC and MFSS depending on requirements for a particular session. Local subscriber directories are stored in the LSCs and network-level worldwide routing tables and addressing and numbering plans are stored in the MFSS.



- Signaling: The local LSC manages ASAC on edge and on access link to the WAN, by preempting and/or blocking both incoming and outgoing sessions.
  - LSC forwards priority of connection request via AS-SIP.
- QoS complements signaling in support of assured services.
  - DSCP assignment as per QoS WG recommendation determines mapping to PHB.
  - The CE uses 4 queues that are bandwidth sized based on traffic-engineered loads:
    - Voice, signaling, & routing in EF queue.
    - Video is placed in an AF queue with two drop probabilities.
    - Preferred data & NM in an AF queue with 2 drop probabilities.
    - Data in an AF queue as Best Effort.
- LSC/ASAC to EBC interface required to indicate which RTS packet flows to allow into the WAN.

LEGEND

AF	Assured Forwarding	EF	Expedited Forwarding	RTS	Real Time Services
ASAC	Assured Service Admission Control	IP	Internet Protocol	VoIP	Voice over Internet Protocol
ASLAN	Assured Services Local Area Network	LSC	Local Session Controller	VVoIP	Voice and Video over IP
AS-SIP	Assured Services Session Initiation Protocol	MFSS	Multifunction Softswitch	WAN	Wide Area Network
CE	Customer Edge Router	NM	Network Management	WG	Working Group
DSCP	Differentiated Services Code Point	PHB	Per-Hop Behavior	XMPP	Extensible Messaging and Presence Protocol
EBC	Edge Boundary Controller	QoS	Quality of Service		



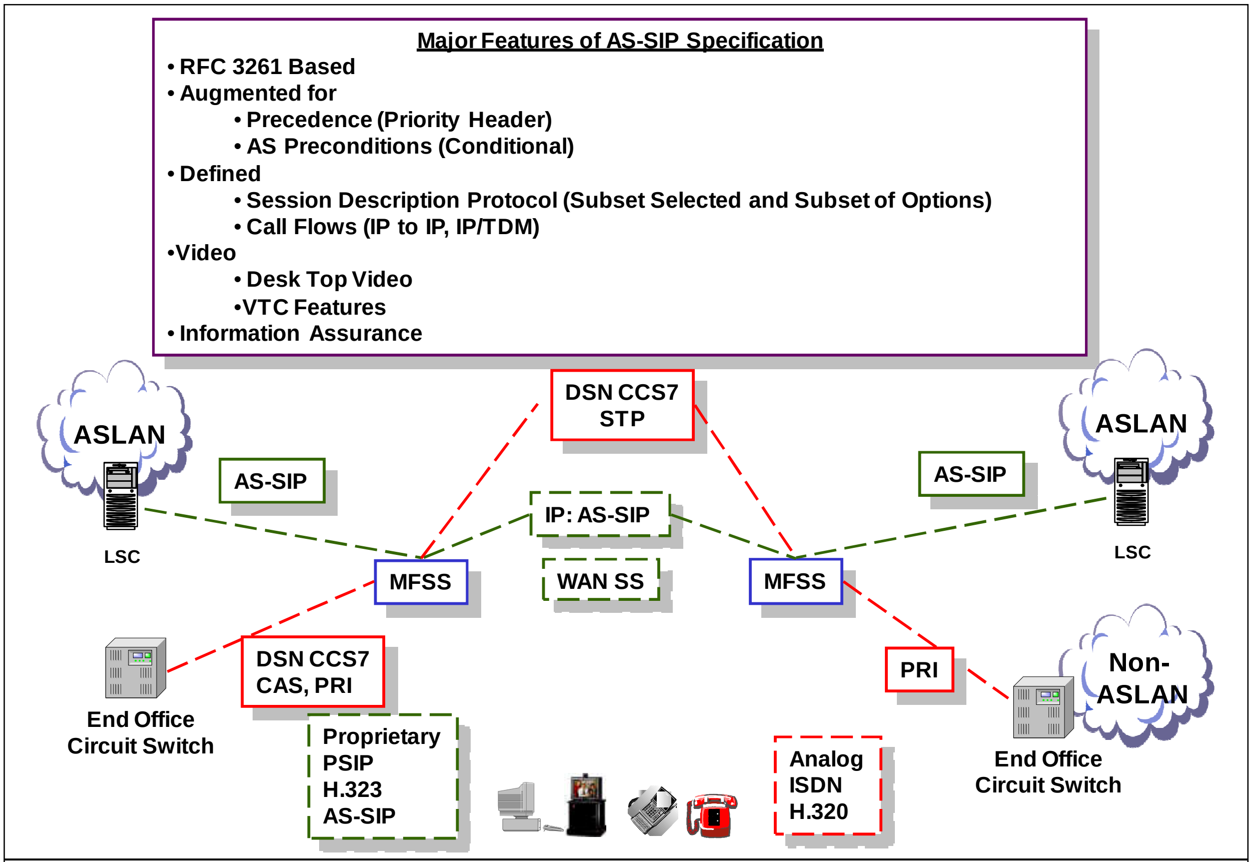
- Signaling: The local LSC manages ASAC on edge and on access link to the WAN, by preempting and/or blocking both incoming and outgoing sessions.
  - LSC forwards priority of connection request via AS-SIP.
- QoS complements signaling in support of assured services.
  - DSCP assignment as per QoS WG recommendation determines mapping to PHB.
  - The CE uses 4 queues that are bandwidth sized based on traffic engineered loads:
    - Voice, signaling, & routing in EF queue.
    - Video is placed in an AF queue with two drop probabilities.
    - Preferred data & NM in an AF queue with 2 drop probabilities.
    - Data in an AF queue as Best Effort.
- LSC/ASAC to EBC interface required to indicate which packet flows to allow into the WAN.

LEGEND					
AF	Assured Forwarding	EF	Expedited Forwarding	PHB	Per Hop Behavior
ASAC	Assured Service Admission Control	EBC	Edge Boundary Controller	QoS	Quality of Service
ASLAN	Assured Services Local Area Network	IP	Internet Protocol	VoIP	Voice over Internet Protocol
AS-SIP	Assured Services Session Initiation Protocol	LSC	Local Session Controller	WAN	Wide Area Network
CER	Customer Edge Router	MFSS	Multifunction Softswitch	WG	Working Group
DSCP	Differentiated Services Code Point	NM	Network Management	XMPP	Extensible Messaging and Presence Protocol

Figure 4.4~~5~~.1-13. Converged VVoIP Design: Signaling, QoS, and Assured Service

4.~~5~~4.1.1.6 Voice and Video Signaling Design

The voice and video signaling design for SBU voice and video is shown in Figure 4.4~~5~~.1-14, SBU Voice and Video Services Signaling Design. For classified voice and video, only the AS-SIP signaling is used since classified VVoIP does not have a TDM legacy infrastructure embedded in the design. During migration, both H.323 and AS-SIP signaling will be used in classified VVoIP. Classified VVoIP interfaces to the TDM DRSN via MGs and SGs. A standalone SS will support AS-SIP signaling in the classified VVoIP network. For SBU voice and video, on the edge of the DISN IP WAN cloud, an LSC on the B/P/C/S signals via AS-SIP to the network-level SS part of the MFSS. The TDM EOs signals via DSN CCS7 to the TDM switching part of the MFSS. The MFSSs use AS-SIP between themselves to set up IP-to-IP EI sessions across the DISN IP WAN.


Major Features of AS-SIP Specification
• RFC 3261 Based
• Augmented for
• Precedence (Priority Header)
• AS Preconditions (Conditional)
• Defined
• Session Description Protocol (Subset Selected and Subset of Options)
• Call Flows (IP to IP, IP/TDM)
•Video
• Desk Top Video
•VTC Features
• Information Assurance
ASLAN
LSC
AS-SIP
DSN CCS7 STP
IP: AS-SIP
MFSS
WAN SS
MFSS
AS-SIP
ASLAN
LSC
End Office Circuit Switch
DSN CCS7 CAS, PRI
Proprietary PSIP H.323 AS-SIP
Analog ISDN H.320
PRI
Non-ASLAN
End Office Circuit Switch

LEGEND

AS	Assured Services	IP	Internet Protocol	RFC	Request for Comment
ASLAN	Assured Services Local Area Network	ISDN	Integrated Services Digital Network	SS	Softswitch
AS-SIP	Assured Services Session Initiation Protocol	LSC	Local Session Controller	STP	Signaling Transfer Point
CAS	Channel Associated Signaling	MFSS	Multifunction Softswitch	TDM	Time Division Multiplexing
CCS7	Common Channel Signaling System No. 7	PRI	Primary Rate Interface	VTC	Video Teleconferencing
DSN	Defense Switched Network	PSIP	Program and System Information Protocol	WAN	Wide Area Network

Figure 4.4~~5~~.1-14. SBU Voice and Video Services Signaling Design

The MFSSs use DSN CCS7 to set up TDM-to-TDM EI sessions across the TDM trunking part of the DISN WAN. Both types of signaling are required to support a hybrid TDM and IP EI environment as the DISN voice and video network migrates to an all IP EI environment in the post-2016 timeframe.

NOTE: The DSN CCS7 network needs to be supported as long as TDM EOs are still connected to the MFSSs. The MILDEPs will control the pace and timing of the phase-out of TDM EOs on the B/P/C/S.

The key rules and attributes of the signaling design are as follows:

1. Two-level signaling hierarchy: LSC and MFSS (or WAN SS).

   a. LSC A to MFSS A to MFSS B to LSC B when the LSCs have different primary MFSSs.

b. LSC A to MFSS A to LSC B when they have the same primary MFSS.

2. The LSCs are assigned a primary and backup MFSS for signaling robustness.

3. Signaling from an IP EI to an LSC may be proprietary, or AS-SIP.

~~4. AS-SIP will be specified in time for 2009 implementation.~~

~~5~~4. The LSC-to-LSC signaling is not permitted external to the security enclave except for use in cases involving deployable products operating in a single area of operational responsibility network that is not the DISN.

~~6~~5. The LSC can set up:

a. On-base sessions when a connection to an MFSS is lost.
b. Sessions to PSTN trunks independent of an MFSS.

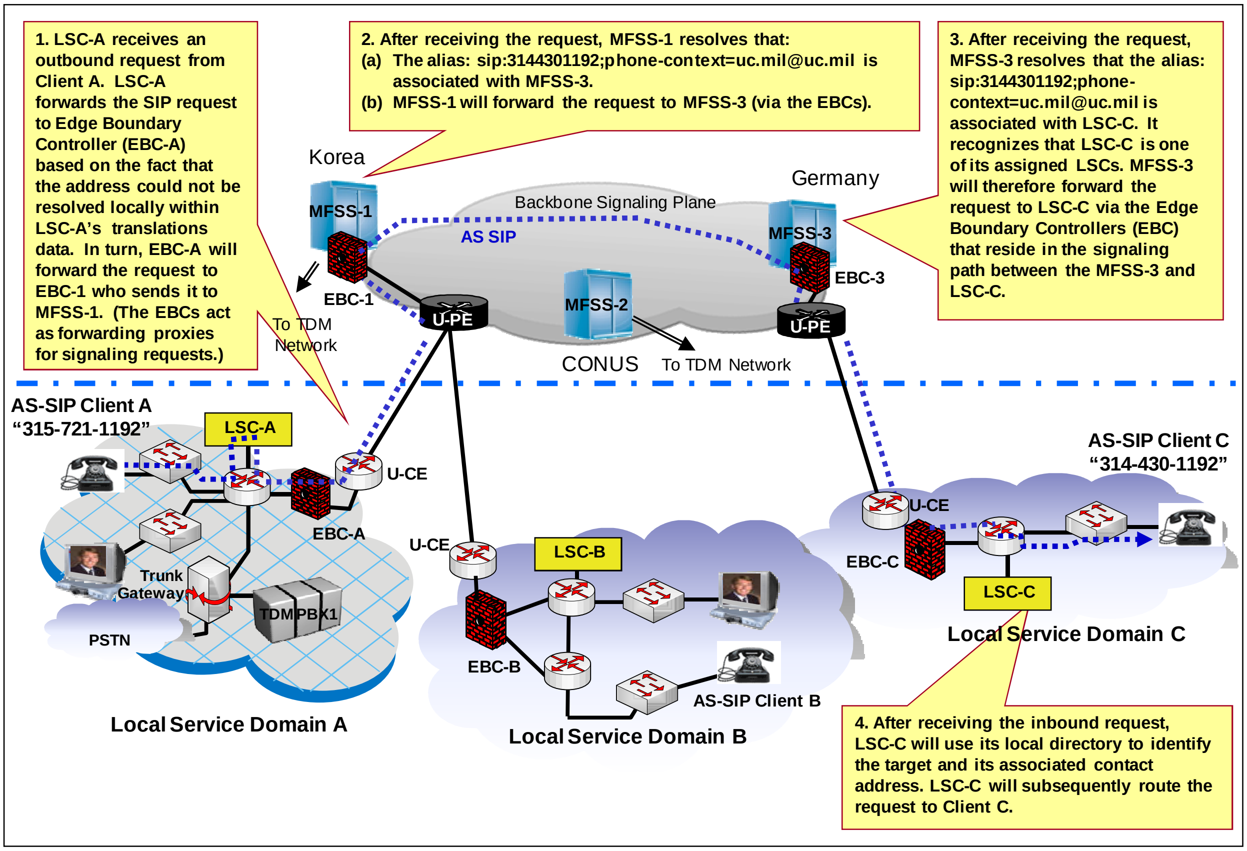
~~7~~6. The LSC and MFSS requirements.

~~8~~7. Signaling.

a. A TDM EO will signal via DSN CCS7, PRI, or CAS to MFSSs.
b. The MFSSs will signal via CAS/PRI to the PSTN and to coalition gateways.

The LSC-to-LSC signaling without a network-level SS for other than deployed Joint Task Forces (JTFs) are under assessment. This assessment is necessary because this configuration has limitations with respect to managing traffic flows from the edge into the network for SA responses of the JTF-GNO NETOPS, and they have visibility limitations (except for cases involving intrabase where an LSC cluster with a master LSC is implemented or for some Services' Deployable Programs under Tailored Information Support Plans (TISPs)). Signaling from the LSC must pass through the network SS part of the MFSS or through a network-level SS so the MFSS/SS can implement Precedence-Based Network Management (PBNM) controls and police the proper use of access circuit bandwidth. For bases that have a collocated MFSS, base-level access to the local PSTN can be provided through the LSC portion of the MFSS. At the network level, the MFSS will serve as the gateway to external networks, such as Services' Deployable Programs networks, the DRSN, and coalition networks, using appropriate signaling protocols, such as CAS/PRI signaling.

The E2E, two-level SBU AS-SIP network signaling design is shown in Figure 4.4~~5~~.1-15, E2E Two-Level SBU AS-SIP Network Signaling Design. For classified networks, the two-level signaling uses WAN SSs rather than MFSSs.



1. LSC-A receives an outbound request from Client A. LSC-A forwards the SIP request to Edge Boundary Controller (EBC-A) based on the fact that the address could not be resolved locally within LSC-A's translations data. In turn, EBC-A will forward the request to EBC-1 who sends it to MFSS-1. (The EBCs act as forwarding proxies for signaling requests.)

2. After receiving the request, MFSS-1 resolves that:
(a) The alias: sip:3144301192;phone-context=uc.mil@uc.mil is associated with MFSS-3.
(b) MFSS-1 will forward the request to MFSS-3 (via the EBCs).

3. After receiving the request, MFSS-3 resolves that the alias: sip:3144301192;phone-context=uc.mil@uc.mil is associated with LSC-C. It recognizes that LSC-C is one of its assigned LSCs. MFSS-3 will therefore forward the request to LSC-C via the Edge Boundary Controllers (EBC) that reside in the signaling path between the MFSS-3 and LSC-C.

4. After receiving the inbound request, LSC-C will use its local directory to identify the target and its associated contact address. LSC-C will subsequently route the request to Client C.

Figure 4.4~~5~~.1-15. E2E Two-Level SBU AS-SIP Network Signaling Design

4.~~5~~4.1.1.7 Information Assurance Design

Information Assurance is a key aspect in the design of any IP-based network. Internet Protocol is inherently vulnerable to eavesdropping and a variety of denial of service (DoS) attacks. Voice and Video over IP introduces avenues of attack due to its use of dynamically assigned User Datagram Protocol (UDP) sessions that cannot be addressed by traditional data firewalls. Therefore, VVoIP are applications that use IP for transport and inherit the threats associated with IP as well as adding vulnerabilities that are unique to the VVoIP technology. A tailored VVoIP Information Assurance design is necessary and is addressed in detail in Section 5.4, Information Assurance Requirements. The major components of the Information Assurance design include the protocols used, the interfaces of LSCs and MFSS to external control devices, and the design of the ASLAN. The methods for securing the VVoIP protocols are illustrated in Figure 4.4~~5~~.1-16, Information Assurance Protocols. Key to the design is a hop-by-hop security model for trust between the signaling appliances using the DoD Public Key Infrastructure (PKI) for authentication.

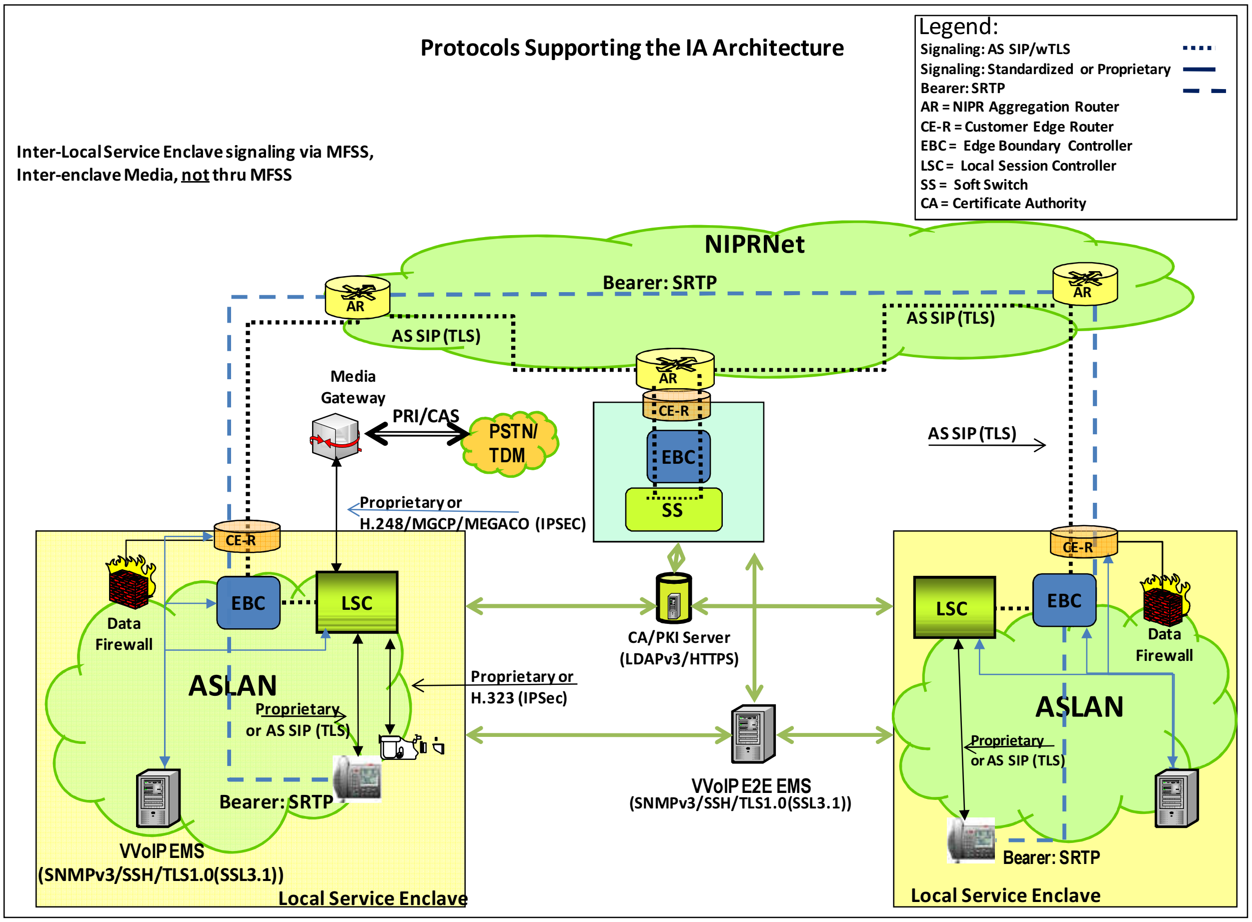
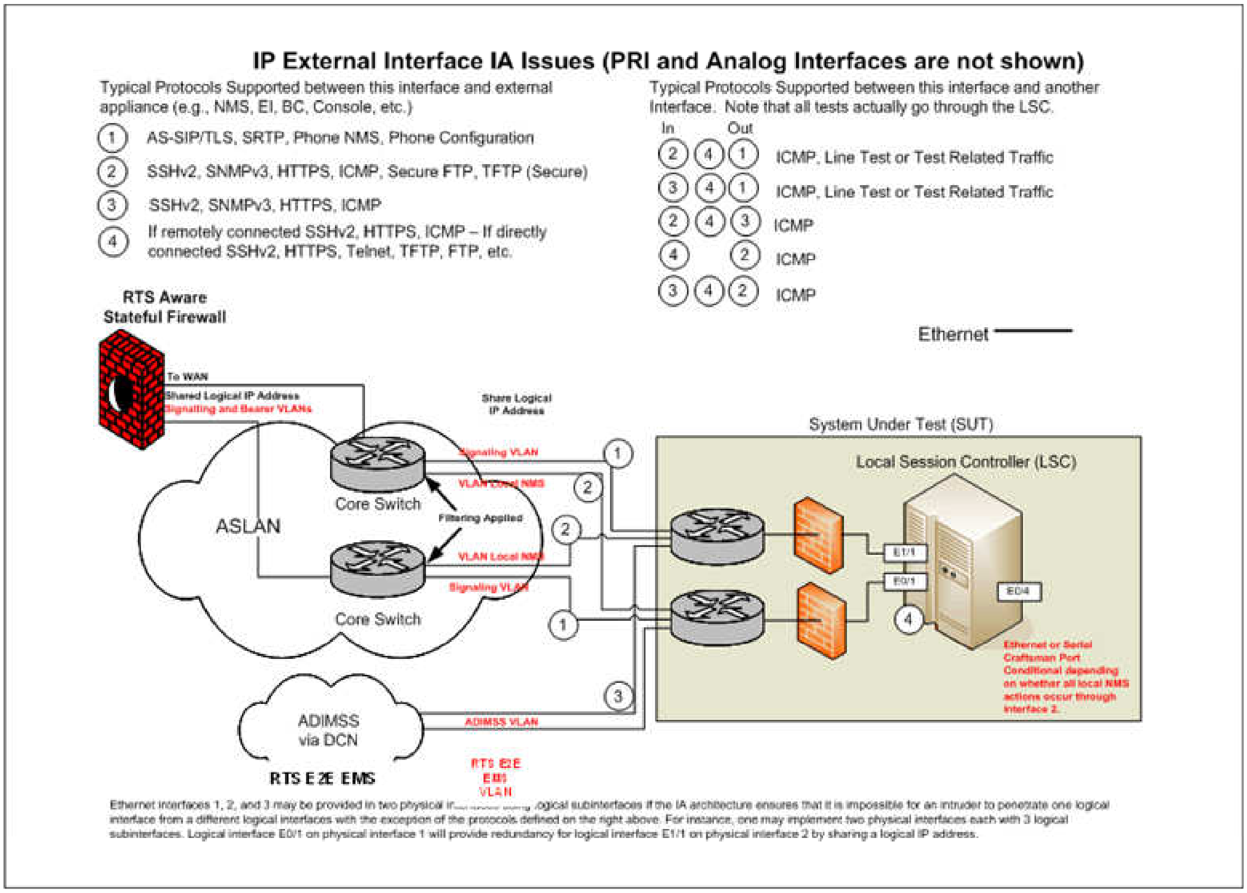

Protocols Supporting the IA Architecture
Legend:
Signaling: AS SIP/wTLS ····
Signaling: Standardized or Proprietary —
Bearer: SRTP – –
AR = NIPR Aggregation Router
CE-R = Customer Edge Router
EBC = Edge Boundary Controller
LSC = Local Session Controller
SS = Soft Switch
CA = Certificate Authority
Inter-Local Service Enclave signaling via MFSS,
Inter-enclave Media, not thru MFSS
NIPRNet
Bearer: SRTP
AR
AR
AR
AS SIP (TLS)
AS SIP (TLS)
Media
Gateway
PRI/CAS
PSTN/
TDM
CE-R
EBC
SS
AS SIP (TLS)
Proprietary or
H.248/MGCP/MEGACO (IPSEC)
CE-R
CE-R
Data
Firewall
EBC
LSC
ASLAN
Proprietary
or AS SIP (TLS)
Bearer: SRTP
VVoIP EMS
(SNMPv3/SSH/TLS1.0(SSL3.1))
Local Service Enclave
CA/PKI Server
(LDAPv3/HTTPS)
Proprietary or
H.323 (IPSec)
VVoIP E2E EMS
(SNMPv3/SSH/TLS1.0(SSL3.1))
LSC
EBC
Data
Firewall
ASLAN
Proprietary
or AS SIP (TLS)
Bearer: SRTP
Local Service Enclave

Figure 4.4~~5~~.1-16. Information Assurance Protocols

Figure 4.4~~5~~.1-17, IP External Interfaces to the LSC or MFSS, illustrates the IP interfaces to the LSC or MFSS to remote access terminals, such as the RTS EMS, local NMS, and the Ethernet connections for signaling and bearer traffic.



IP External Interface IA Issues (PRI and Analog Interfaces are not shown)

Typical Protocols Supported between this interface and external appliance (e.g., NMS, EI, BC, Console, etc.)

1. AS-SIP/TLS, SRTP, Phone NMS, Phone Configuration
2. SSHv2, SNMPv3, HTTPS, ICMP, Secure FTP, TFTP (Secure)
3. SSHv2, SNMPv3, HTTPS, ICMP
4. If remotely connected SSHv2, HTTPS, ICMP – If directly connected SSHv2, HTTPS, Telnet, TFTP, FTP, etc.

Typical Protocols Supported between this interface and another Interface. Note that all tests actually go through the LSC.

In		Out	
2	4	1	ICMP, Line Test or Test Related Traffic
3	4	1	ICMP, Line Test or Test Related Traffic
2	4	3	ICMP
4		2	ICMP
3	4	2	ICMP

Ethernet interfaces 1, 2, and 3 may be provided in two physical i[illegible] logical subinterfaces if the IA architecture ensures that it is impossible for an intruder to penetrate one logical interface from a different logical interfaces with the exception of the protocols defined on the right above. For instance, one may implement two physical interfaces each with 3 logical subinterfaces. Logical interface E0/1 on physical interface 1 will provide redundancy for logical interface E1/1 on physical interface 2 by sharing a logical IP address.

Figure 4.4~~5~~.1-17. IP External Interfaces to the LSC or MFSS

Figure 4.4~~5~~.1-18, ASLAN Enclave Boundary Security Diagram, depicts a diagram of the Information Assurance design needed as part of the ASLAN. The key feature of Figure 4.4~~5~~.1-18 is the need for two types of firewalls: one for data traffic and another for VVoIP traffic. The voice and/or video signaling packets and media stream packets must traverse the edge boundary control device that implements a voice and/or video dynamic stateful AS-SIP aware application firewall, which provides Network Address Translation (NAT), MFSS failover, and port pinholes for individual voice and video sessions. A UC APL product called an Edge Boundary Controller (EBC) consisting of the voice and/or video firewall/border controller, has been defined and specified in Section 5.3.2, Assured Services Requirements.

The requirements for the Information Assurance functionality are provided in Section 5.4, Information Assurance Requirements, which dictates the detailed methods by which all known security threats against the network have been mitigated.

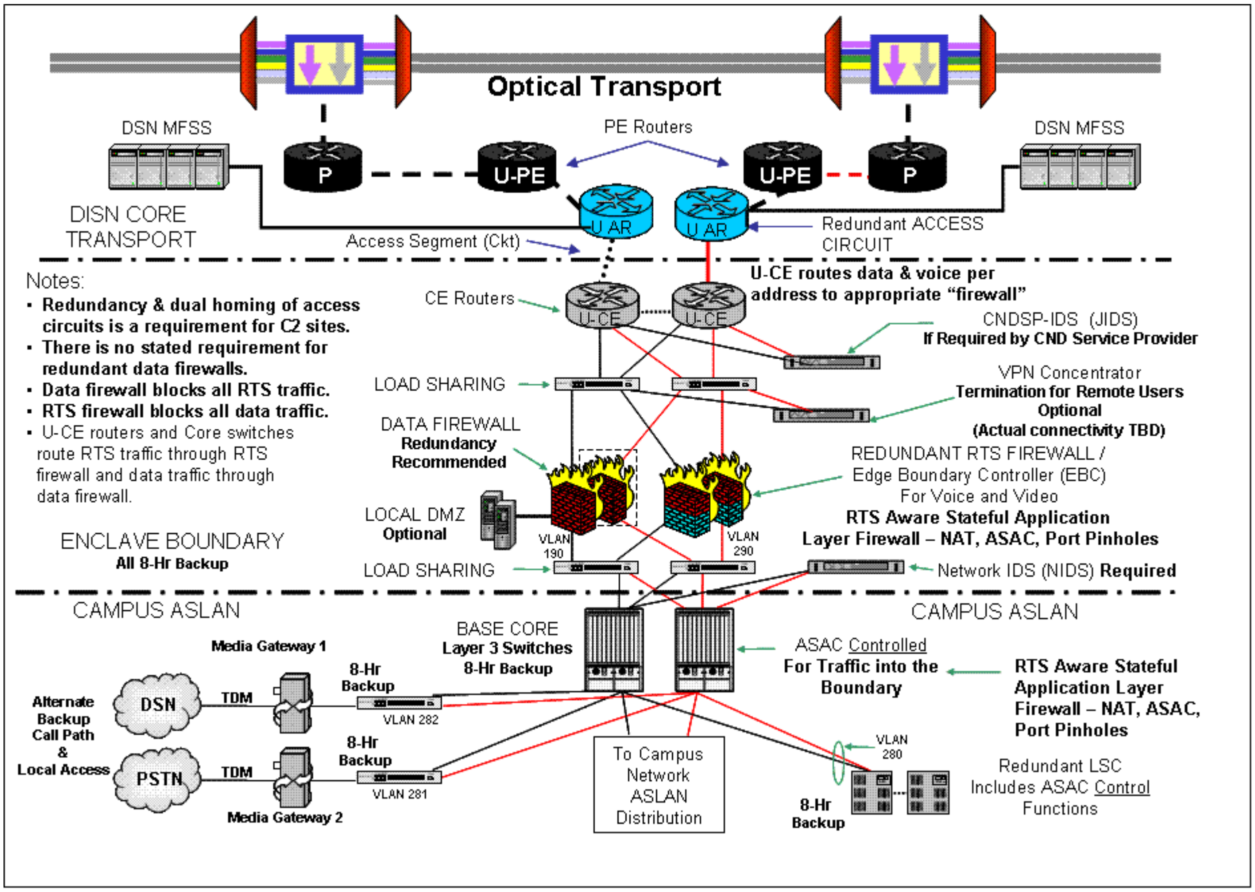
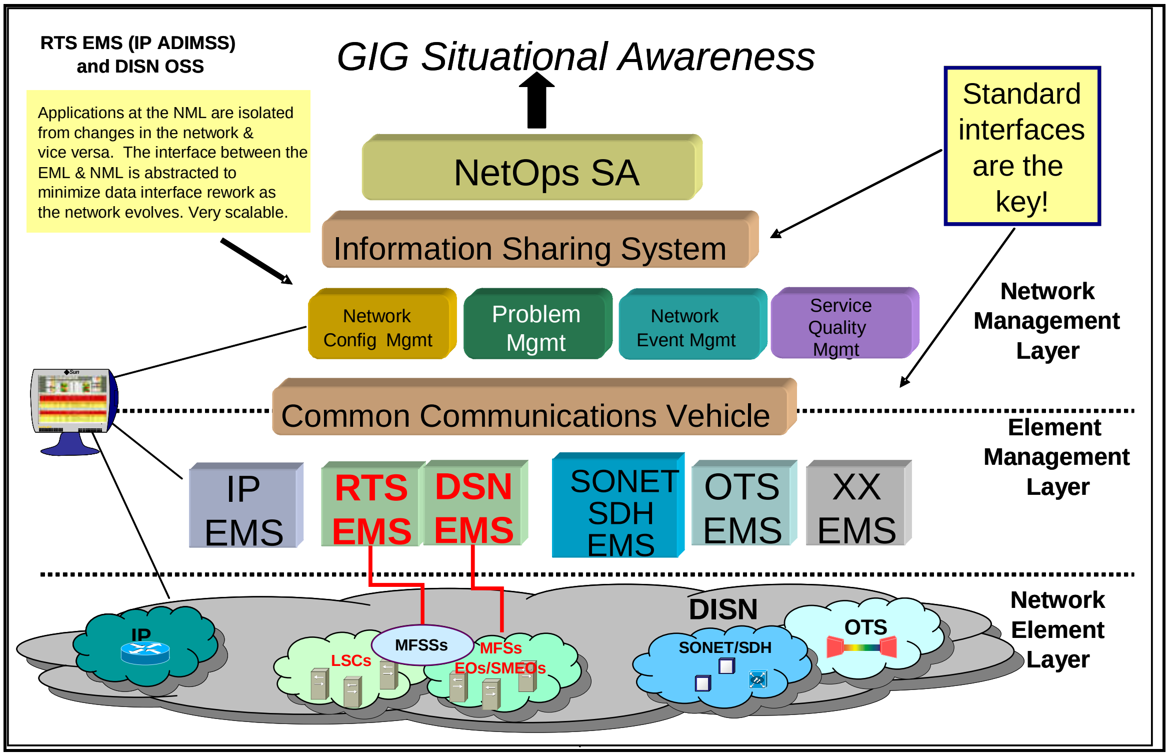


Figure 4.4~~5~~.1-18. ASLAN Enclave Boundary Security Design

4.~~5~~4.1.1.8 Network Management Design

Network management of the VVoIP services E2E is a critical component of NETOPS. Since the VVoIP network will be a hybrid network for an extended period, the NMS must continue to be provided by an EMS via commanding and monitoring of the voice and video services for both circuit-switched and IP technologies as part of the DISN OSS. This hybrid operation within the DISN Operational Support System (OSS) is illustrated in Figure 4.4~~5~~.1-19, Role of E2E RTS EMS in DISN OSS, where the EMS is shown at the bottom of the DISN OSS hierarchy.

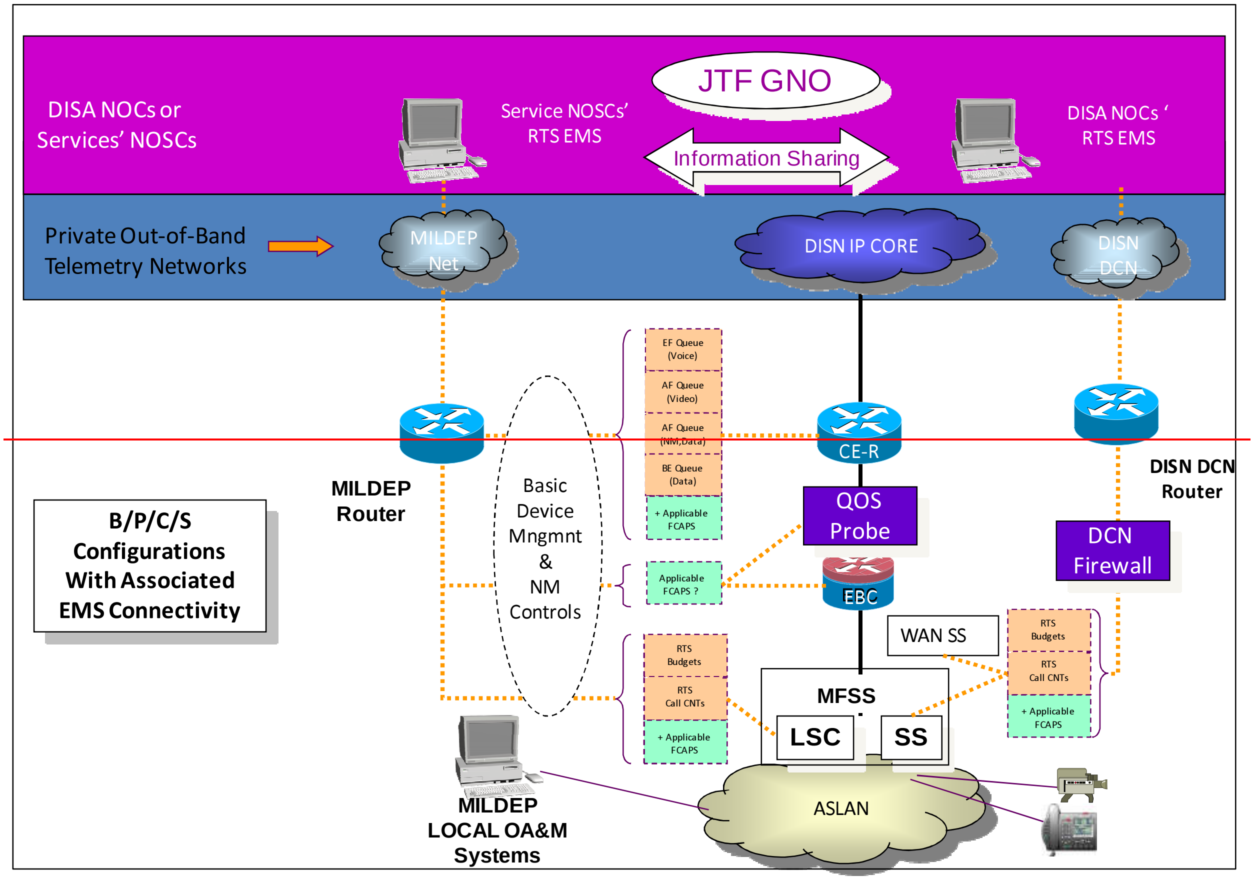


Applications at the NML are isolated from changes in the network & vice versa. The interface between the EML & NML is abstracted to minimize data interface rework as the network evolves. Very scalable.

Figure 4.4~~5~~.1-19. Role of RTS EMS in DISN OSS

In support of the Joint CONOPS for shared SA, and as an enabler of Net-Centric GIG Enterprise Management (GEM), the DoD Component EMS and RTS EMS must provide new ~~machine-to-machine~~web services interfaces for "reading and writing" to the Services' NMS to support the JTF-GNO in both visibility and reconfiguration of the network, and in controlling the flow of sessions. The design for support of JTF-GNO is illustrated in Figure 4.4~~5~~.1-20, RTS EMS Role in Providing E2E EMS. Since the RTS EMS is Government Off-the-Shelf (GOTS) based on COTS, it is available for the MILDEPs to use at their NOCs as well.

~~{Review/update requested from Cossaboom}~~


DISA NOCs or
Services' NOSCs
Service NOSCs'
RTS EMS
JTF GNO
Information Sharing
DISA NOCs '
RTS EMS
Private Out-of-Band
Telemetry Networks
MILDEP
Net
DISN IP CORE
DISN
DCN
EF Queue
(Voice)
AF Queue
(Video)
AF Queue
(NM,Data)
BE Queue
(Data)
+ Applicable
FCAPS
MILDEP
Router
Basic
Device
Mngmnt
&
NM
Controls
CE-R
QOS
Probe
DISN DCN
Router
DCN
Firewall
B/P/C/S
Configurations
With Associated
EMS Connectivity
Applicable
FCAPS ?
EBC
WAN SS
RTS
Budgets
RTS
Call CNTs
+ Applicable
FCAPS
MFSS
LSC
SS
RTS
Budgets
RTS
Call CNTs
+ Applicable
FCAPS
ASLAN
MILDEP
LOCAL OA&M
Systems

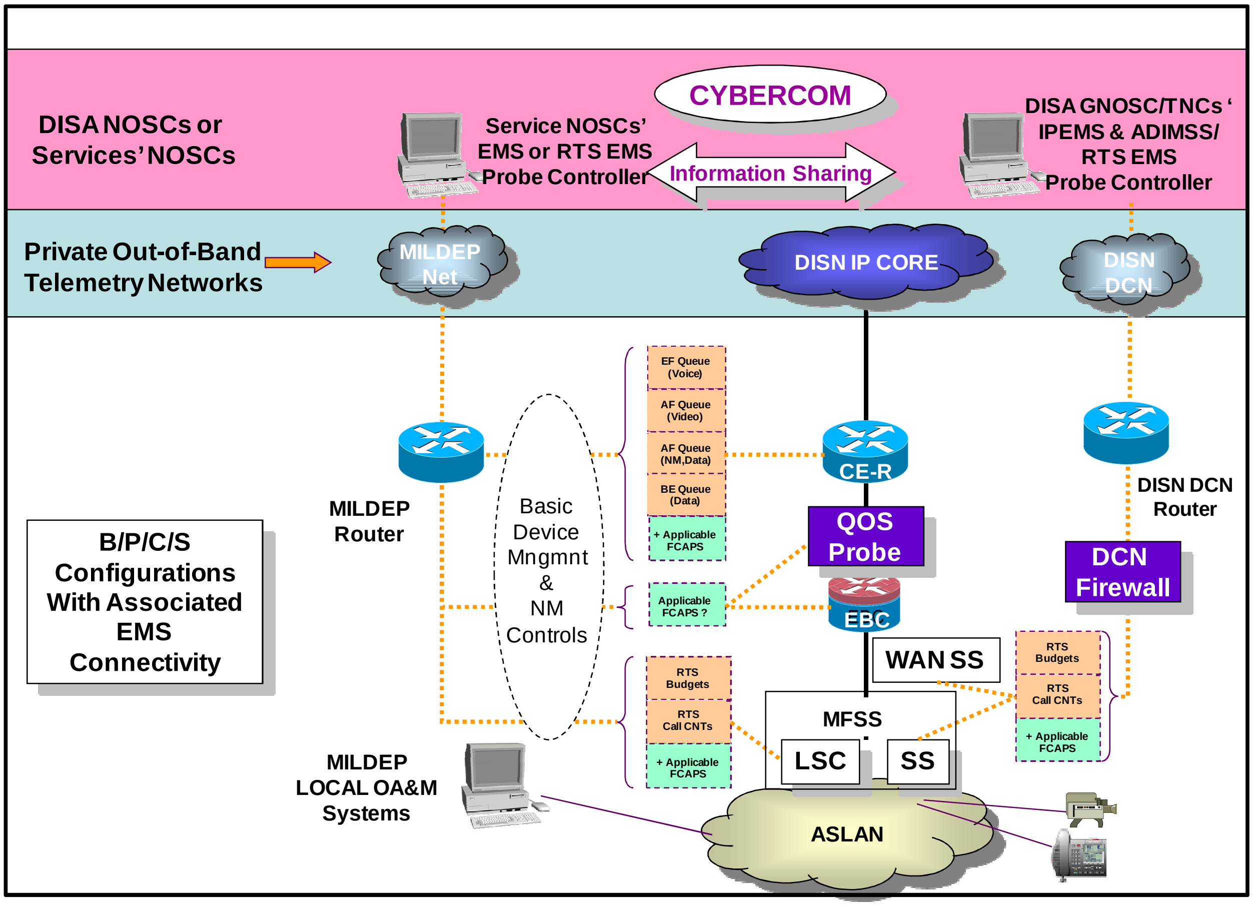


Figure 4.4~~5~~.1-20. RTS EMS Role in Providing E2E GEM

4.4.1.1.9 Enterprise –wide Design

The enterprise-wide design is illustrated in Figure 4.4.1-21. This design consists of an Enterprise Service node location from which a centrally located LSC and MCU provide UC service to several geographically separated local service enclaves. It must be noted that the local service enclaves are separate security enclaves connected by the DISN Core. Access to the PSTN is provided directly from each local service enclave via remote media gateways controlled by the enterprise LSC. This design can provide a minimal footprint at the MILDEP level, offer savings in O&M and space requirements, allows MILDEPS to invest in bandwidth and diversity in lieu of telcom equipment. The centralized design can provide a tighter integration with DISN enterprise collaboration, directory services, and conferencing offerings.

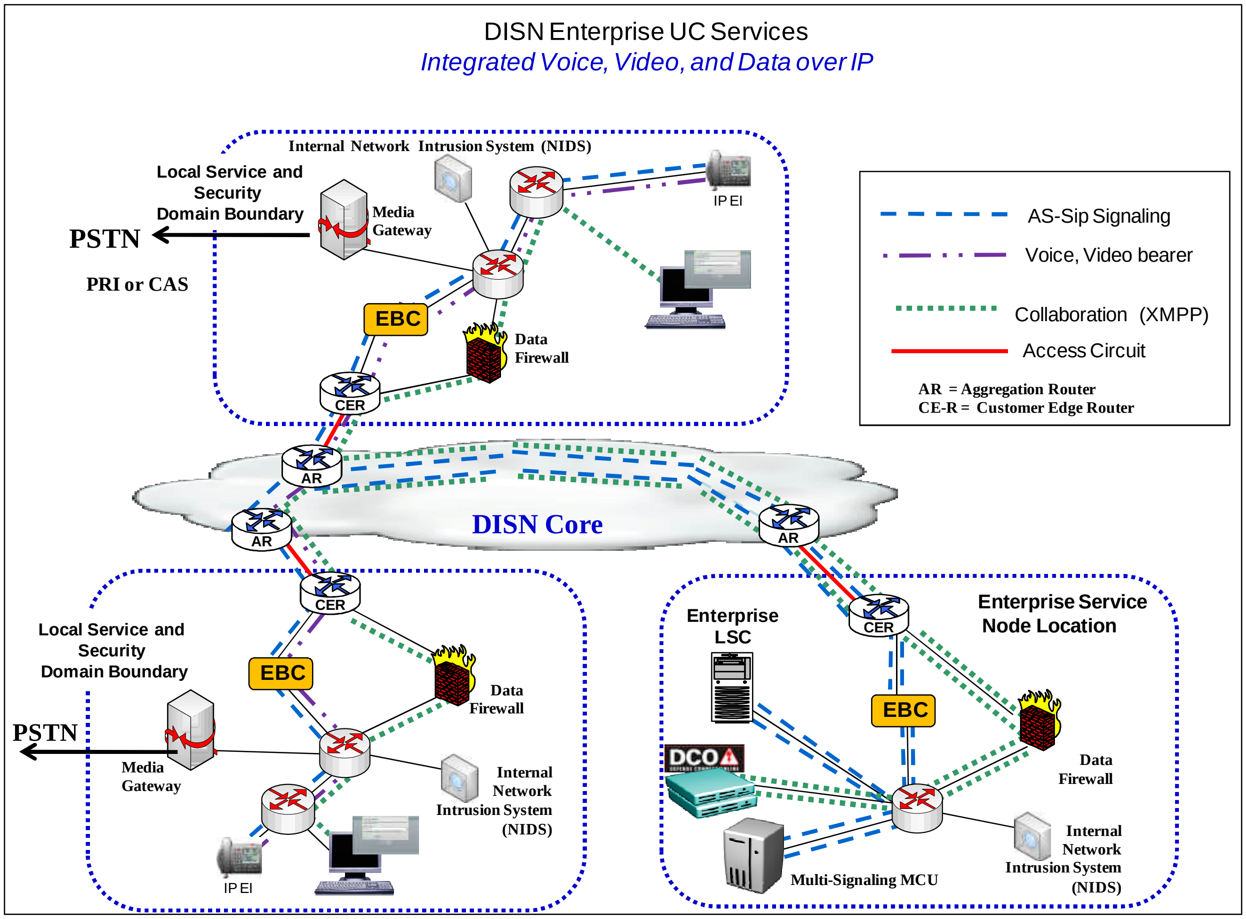

DISN Enterprise UC Services
Integrated Voice, Video, and Data over IP
Internal Network Intrusion System (NIDS)
Local Service and Security Domain Boundary
PSTN
PRI or CAS
Media Gateway
IP EI
EBC
Data Firewall
CER
AR
DISN Core
AS-Sip Signaling
Voice, Video bearer
Collaboration (XMPP)
Access Circuit
AR = Aggregation Router
CE-R = Customer Edge Router
Local Service and Security Domain Boundary
PSTN
EBC
Data Firewall
Media Gateway
Internal Network Intrusion System (NIDS)
IP EI
Enterprise LSC
Enterprise Service Node Location
CER
EBC
DCO
Data Firewall
Internal Network Intrusion System (NIDS)
Multi-Signaling MCU

Figure 4.4.1-21. DISN Enterprise UC Services Concept

~~4.4.1.1.9 Enterprise System Design for Voice and Video Services~~

~~{Barry and John R. to provide information.}~~

~~*4.45.1.2 Relationship between UC Network Description and Products to be Tested for APL Certification*~~

~~{Jo – Updated with new products.}~~

~~This section describes relationships between voice and video architectural components, appliance functions, and UC products to be tested for APL certification. The term “appliance function” is introduced because the IP-based UC APL products will often consist of software functions and features (e.g., appliances) that are distributed over several hardware components connected over a network infrastructure (e.g., LAN), while a TDM-based APL product, such as~~

~~an EO, consists of a single unit containing all required telephony functions. Appliances operate at the signaling, bearer, and NM planes. Appliance functions are described and referred to throughout the UCR, but are not considered products for UC APL certification, but rather functions and features that form a part of a UC APL product. Table 4.45.1-2, Summary of IP-Based Appliances and UC APL Products, provides a summary of IP-based appliances and APL products.~~

~~Table 4.45.1-2. Summary of IP-Based Appliances and UC APL Products~~

~~**ITEM**~~	~~**ITEM CATEGORY**~~	~~**ROLE AND FUNCTIONS**~~
~~End Instrument (EI)~~	~~Appliance~~	~~Appliance part of LSC~~
~~AS-SIP End Instrument (AEI)~~	~~APL Product~~	~~Product consisting of a single appliance~~
~~Media Gateway (MG)~~	~~Appliance~~	~~Media conversion function as part of the LSC and MFSS~~
~~Signaling Gateway (SG)~~	~~Appliance~~	~~Signaling conversion function as part of the LSC and MFSS~~
~~AS-SIP Signaling Appliance~~	~~Appliance~~	~~Appliance function within and LSC and MFSS that provides AS-SIP signaling capability~~
~~Call Connection Agent (CCA)~~	~~Appliance~~	~~Appliance function within an LSC and MFSS that performs parts of session control and signaling functions~~
~~Registrar~~	~~Appliance~~	~~Appliance function that stores the location of a registrant and its profile~~
~~Registrant~~	~~Appliance~~	~~Appliance function used to register with the network to seek and gain authority to invoke services or resources from the network~~
~~LAN Switch/Router (Access, Distribution, and Core)~~	~~APL Products~~	~~APL products used in an ASLAN~~
~~Secure End Instrument (SEI)~~	~~APL Product~~	~~Product consisting of a single appliance~~
~~Local Session Controller (LSC)~~	~~APL Product~~	~~Product providing many local telephony functions~~
~~Multifunction Softswitch (MFSS)~~	~~APL Product~~	~~Large, complex product providing many local and WAN-related telephony functions~~
~~Wide Area Network Softswitch (WAN SS)~~	~~APL product~~	~~A standalone APL product that acts as an AS-SIP B2BUA within the UC architecture. It provides the equivalent functionality of a commercial SS and has similar functionality to the SS component of an MFSS.~~
~~Dual-Signaling Softswitch (DSSS)~~	~~APL product~~	~~A WAN SS used in the classified network that has both H.323 and AS-SIP signaling~~
~~Dual-Signaling Multipoint Control Unit (DSMCU)~~	~~APL product~~	~~APL product that supports multiple video conferencing signaling protocols, H.320, H.323, and AS-SIP~~
~~Edge Boundary Controller (EBC)~~	~~APL Product~~	~~Product providing firewall functions~~
~~Customer Edge (CE) Router~~	~~APL Product~~	~~Product providing routing functions at the enclave boundary~~
~~DISN WAN Provider (P)/Provider Edge (PE) Router~~	~~APL Product~~	~~Product providing routing of IP packets~~
~~DISN Multi-Service Provisioning Platforms (MSPP)~~	~~APL Product~~	~~Product providing transport access to the DISN WAN~~
~~M13 Multiplexer~~	~~APL Product~~	~~Product providing transport interface to the DISN~~
~~DISN Optical Switch~~	~~APL Product~~	~~Product serving as an optical transport node~~

~~4.45.1.3 Role of LSCs as Replacement for Existing Switching Systems~~

~~When an LSC is placed on the APL, it is also listed as a PBX1 until UCR 2008 expires without additional testing. Going forward, all existing local B/P/C/S TDM switching systems (e.g., PBX2, PBX1, SMEO, and EO) will eventually be phased out and replaced by LSCs.~~

4.4~~5~~.1.~~4~~2 Classified VoIP Network Design

~~{Update – EBC role – need diagram~~
~~Need WAN SS diagram}~~

Figure 4.4~~5~~.1~~-21~~.2-1, Classified VoIP Network Design Illustration, illustrates the classified VoIP design. The approved product types are the same as the SBU approved product types with the exception of the MFSS, which is not needed for classified VoIP and is replaced with a dual-signaling WAN SS capable of both H.323 and AS-SIP signaling, which is described in Section 6.2, Unique Classified Requirements.

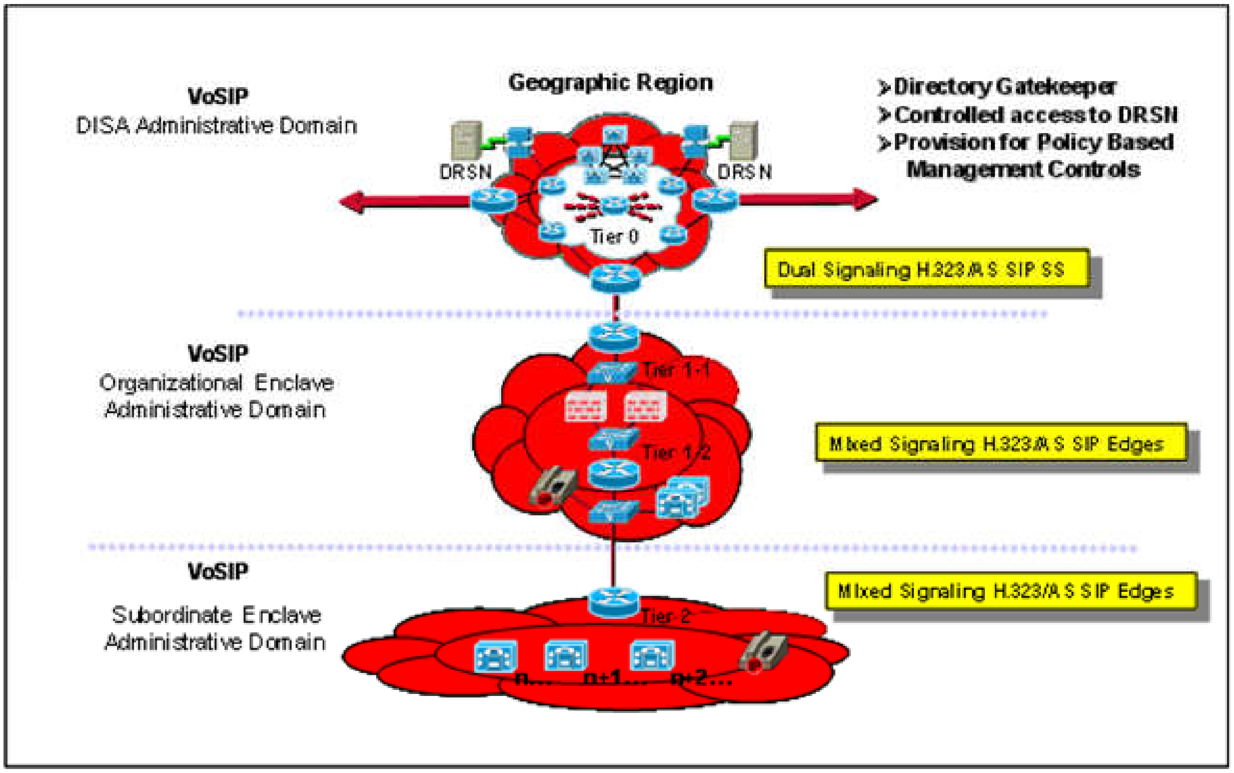

VoSIP
DISA Administrative Domain
Geographic Region
DRSN
DRSN
Tier 0
➢Directory Gatekeeper
➢Controlled access to DRSN
➢Provision for Policy Based Management Controls
Dual Signaling H.323/AS SIP SS
VoSIP
Organizational Enclave Administrative Domain
Tier 1-1
Tier 1-2
Mixed Signaling H.323/AS SIP Edges
VoSIP
Subordinate Enclave Administrative Domain
Tier 2
n…
n+1…
n+2…
Mixed Signaling H.323/AS SIP Edges

Figure 4.4~~5~~.1.2-~~2~~1. Classified VoIP Network Design Illustration

4.4~~5~~.1.~~5~~3 VTC Network Design

DISA provides VTC services as part of the DVS program for joint operations and the MILDEPs have their own VTCs for their unique COIs. The current Video Teleconferencing over IP (VTCoIP) E2E over both the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet) does not provide assured services. The current DoD VTC services use an IP signaling protocol, called H.323, that does not provide Assured Services. They also support video using a TDM protocol, H.320. Due to DoD Components' budgetary constraints and because the VTCoIP technology insertion must be determined by site-by-site business cases, current versions of DVS VTC and MILDEP VTC technologies will provide voice and video services over the DISN for many years. Therefore, the current DVS and MILDEP Multipoint Conferencing Units (MCUs), which use H.320 and H.323, will be augmented to become Dual Signaling MCUs (DSMCUs) supporting interoperability among H.323 and AS-SIP Edge video systems. Figure 4.~~5.1-22~~4.1.3-1, DISN Dual Signaling MCU Design, illustrates the dual IP signaling involved in the VTC networks with backward compatibility to TDM video and the role of the DSMCU in that signaling.

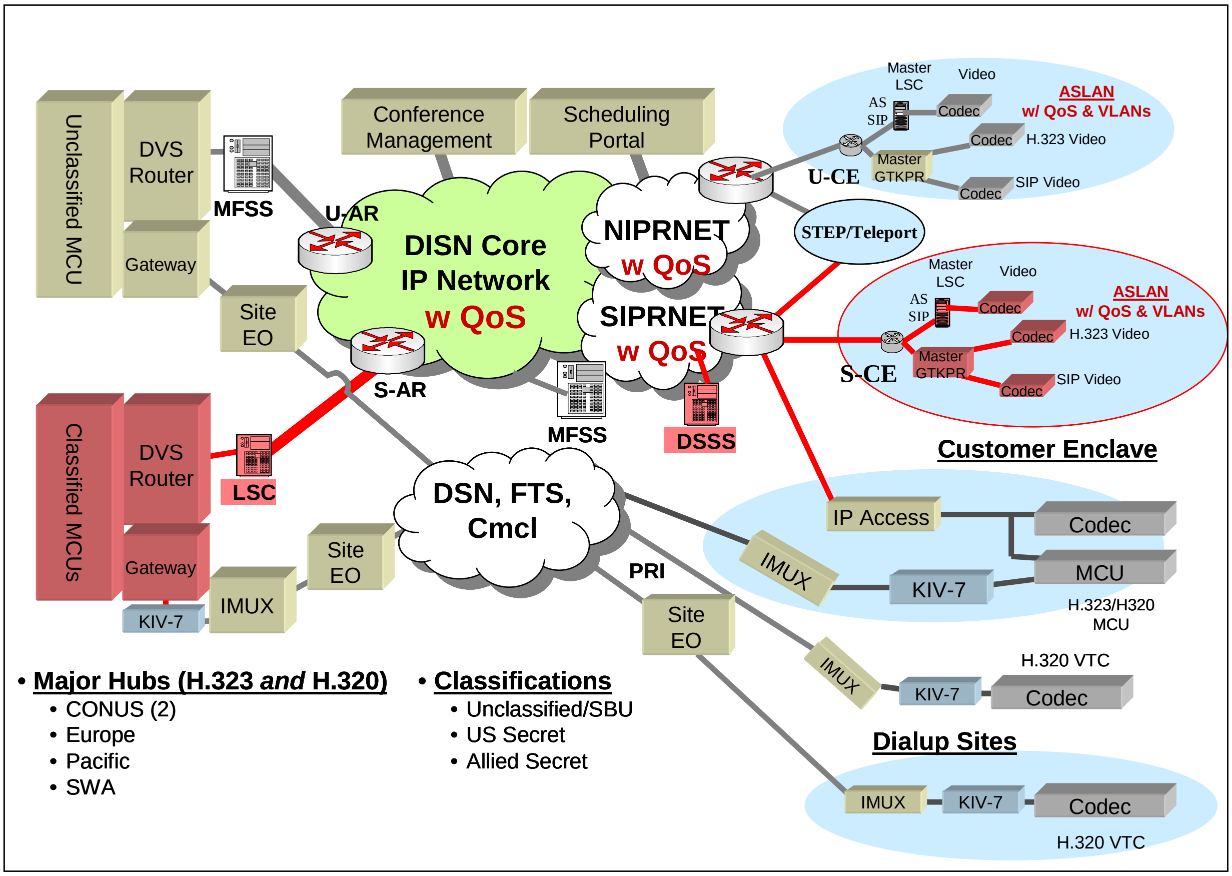


Figure 4.4~~5~~.1.3-~~22~~1. DISN DSMCU Design Hybrid Operations

The DSMCU is an enabling technology for the migration to classified and SBU assured services VTC. The VTC service needs a signaling protocol to establish assured VTCoIP sessions E2E among multiple vendors. The signaling protocol for VTCoIP is AS-SIP. The DSMCU will support the needs of both DISA and MILDEP to migrate from non-assured services to assured services. These DSMCUs will perform all signaling conversions needed to enable legacy H.320, H.323, and AS-SIP technology networks to set up video sessions among DoD Component sites with either non-assured or assured IP signaling technologies. The DSMCUs will support both classified VTC on SIPRNet and SBU VTC on NIPRNet.

4.4~~5~~.1.~~6~~4 DISN Router Hierarchy

Figure 4.4~~5~~.1.4-1~~23~~, DISN Router Hierarchy, illustrates the DISN router hierarchy for FY 2009 for both the unclassified network and the classified network. At this point, the NIPRNet and SIPRNet routers have been transformed to be U-ARs and classified ARs connected to the Unclassified Provider Edge (U-PE) Routers and classified Provider Edge (C-PE) Routers.

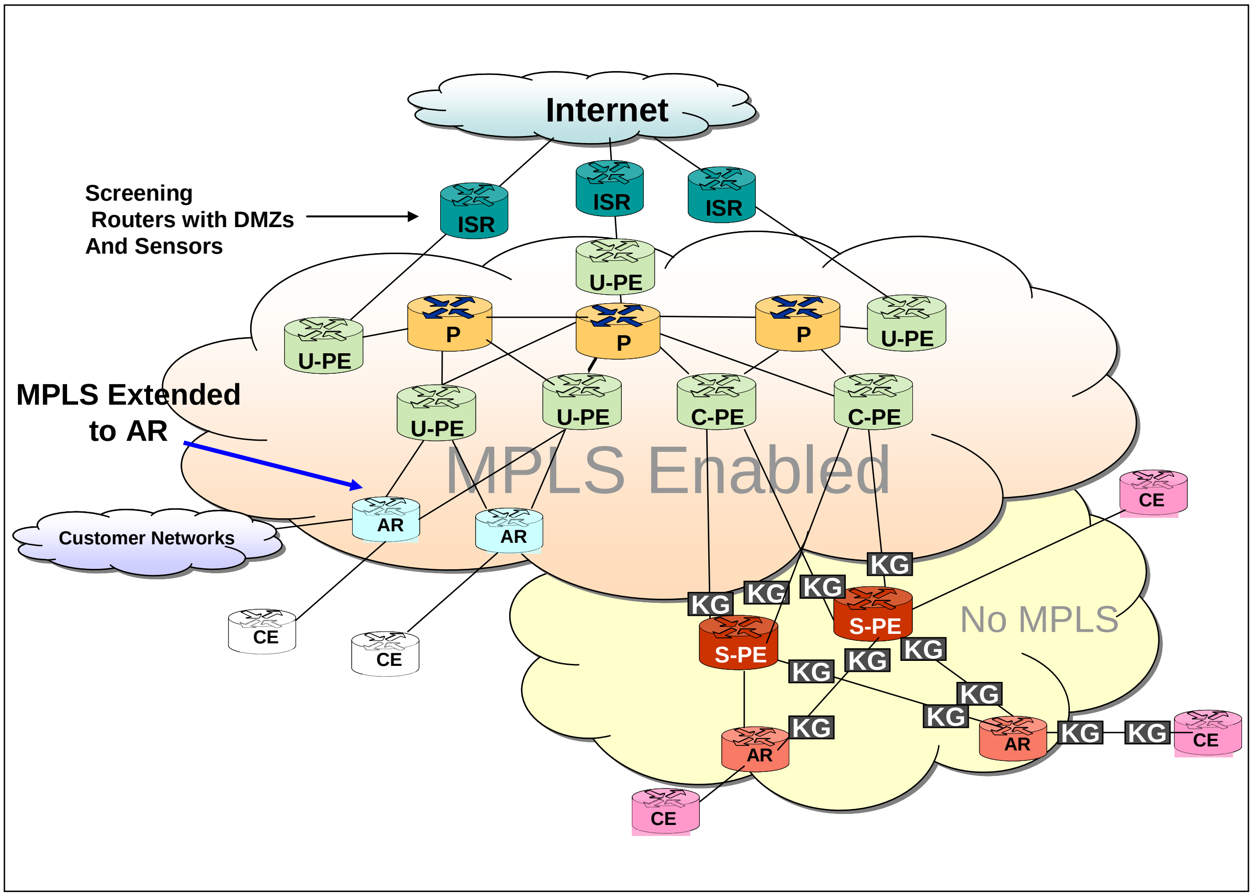


Figure 4.4~~5~~.1.4-~~23~~1. DISN Router Hierarchy

4.4~~5~~.1.~~7~~5 IPv6 Network Design

Figure 4.4~~5~~.1.5-~~2~~1~~4~~, IPv6 Design for SBU and Classified VVoIP, depicts the Internet Protocol version 6 (IPv6) network design for SBU and classified VVoIP and includes the DISN SDNs. All UC approved products will be IPv6 capable, and the VVoIP network will be an IPv6-enabled network during Spiral 2 of its capabilities deployments.

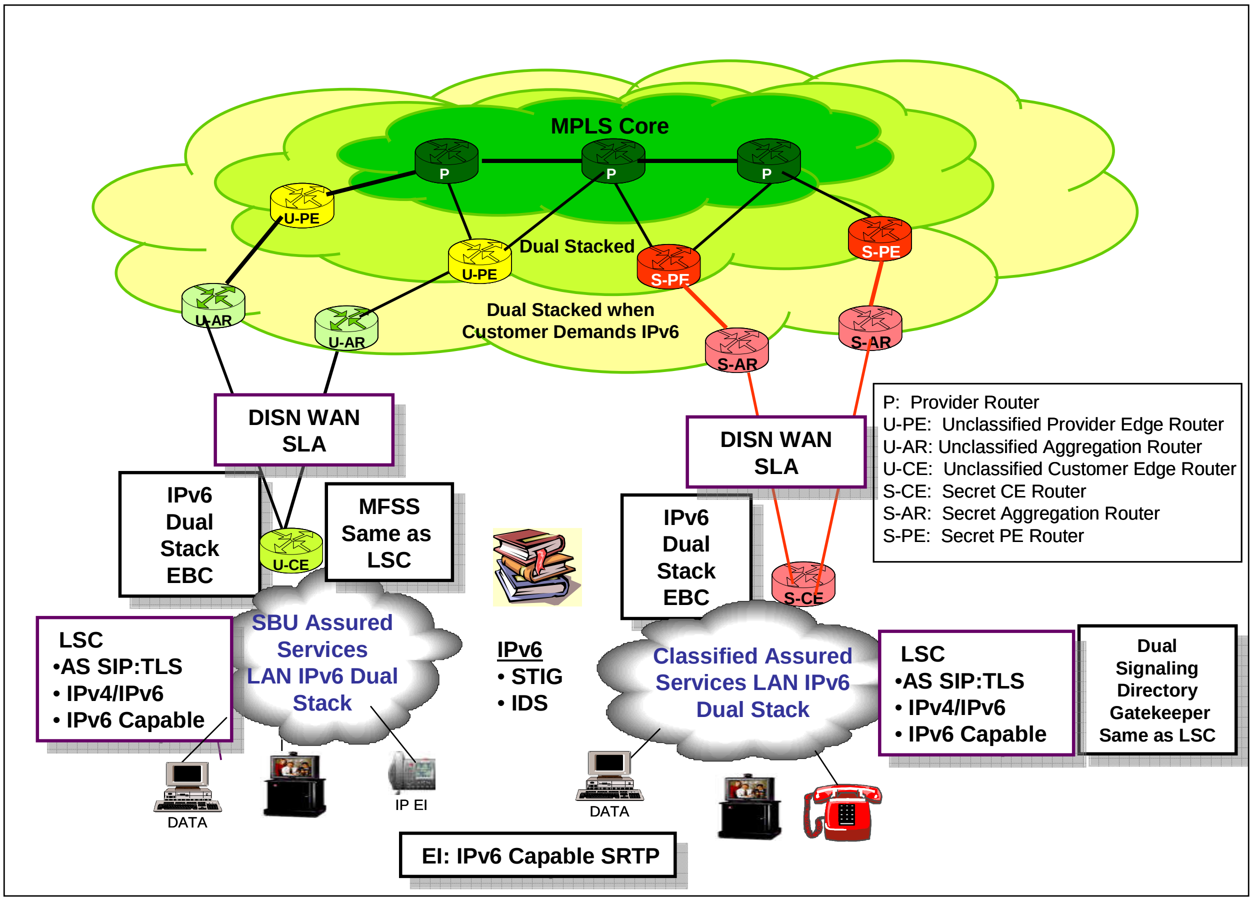


Figure 4.4~~5~~.1.5-~~24~~1. IPv6 Design for SBU and Classified VVoIP

4.4~~5~~.2 ~~Unified Communications~~ Voice, Video and Data Integrated Design for UC

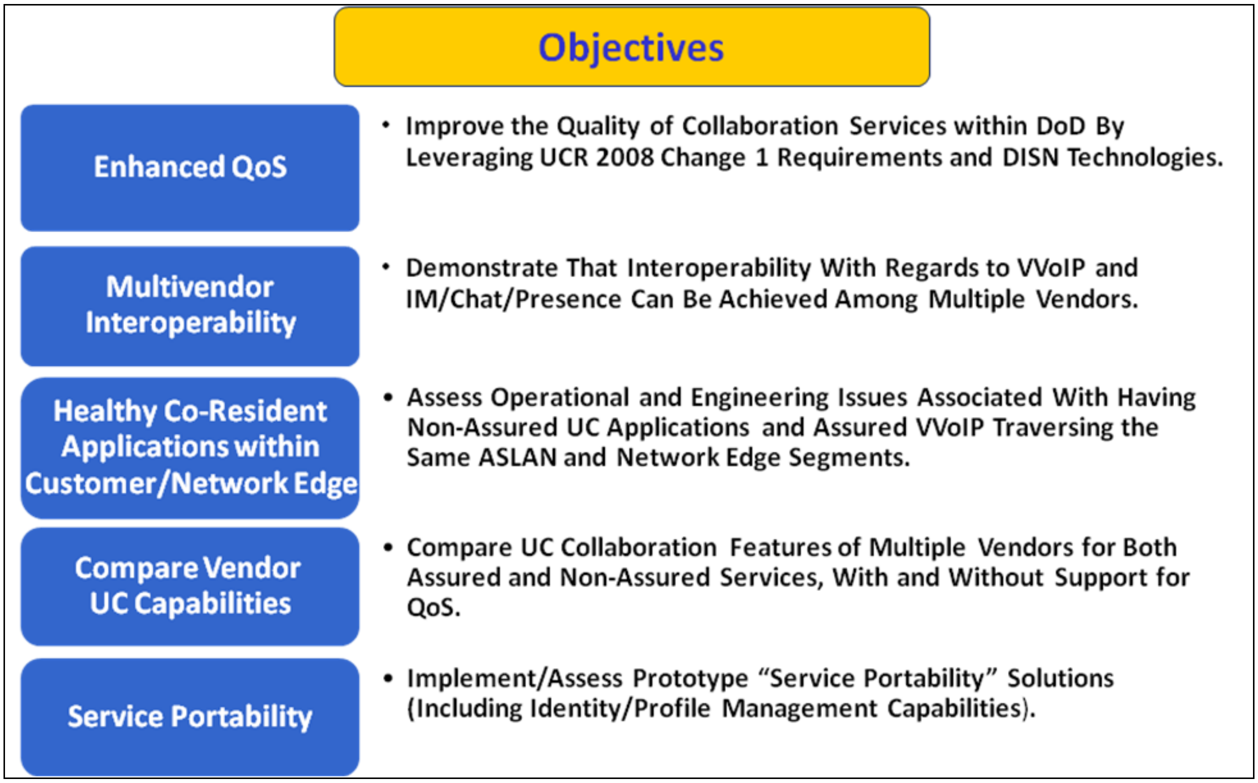
UC services are driven by emerging IP and changing communications technologies, which recognizes evolving communication capabilities from point-to-point to multipoint, voice-only to rich-media, multiple devices to single device, wired to wireless, non-real time to real time, and scheduled to ad hoc~~{intro that references – address different combinations voice, video and data services identified in Section 4.2. Explain the 2 sections (4.5.2.1 integration of this set of services, 4.5.2.2 integration of the 2nd set of services.}~~.

4.4.2.1 Integration of Voice, Video, and Data (Web Conferencing, Web Collaboration, Instant Messaging and Chat, and Presence)

This section provides an overview of the initial system concepts for ~~{title}~~integration of UC services~~UC associated with network-wide collaboration services~~. The voice, video and data ~~UC Collaboration~~ services include multimedia or cross-media collaboration capabilities (including audio collaboration, video collaboration, text-based collaboration, and presence). The focus of the integration ~~UC network-wide collaboration services~~ is to go beyond local, intraenclave test events to implement and assess collaboration services and applications on an E2E, WAN-level basis. These UC network-wide collaboration services raise the need for new designs to address any potential performance, Information Assurance, or engineering/configuration issues associated with these different applications traversing the same ASLAN and Network Edge Segments.~~ {updated by J. Rutledge with new charts, diagrams, ..} All titles lined up 4.5.2.~~

~~*4.5.2.1 UC Network-wide Collaboration Services*~~

Leveraging the UCR 2010, capabilities, the key UC network-wide collaboration services objectives are listed in Figure 4.4~~5~~.2-1, UC Network-wide Collaboration Services Objectives.



Objectives

Enhanced QoS

- Improve the Quality of Collaboration Services within DoD By Leveraging UCR 2008 Change 1 Requirements and DISN Technologies.

Multivendor Interoperability

- Demonstrate That Interoperability With Regards to VVoIP and IM/Chat/Presence Can Be Achieved Among Multiple Vendors.

Healthy Co-Resident Applications within Customer/Network Edge

- Assess Operational and Engineering Issues Associated With Having Non-Assured UC Applications and Assured VVoIP Traversing the Same ASLAN and Network Edge Segments.

Compare Vendor UC Capabilities

- Compare UC Collaboration Features of Multiple Vendors for Both Assured and Non-Assured Services, With and Without Support for QoS.

Service Portability

- Implement/Assess Prototype "Service Portability" Solutions (Including Identity/Profile Management Capabilities).

Figure 4.4~~5~~.2-1. UC Network-Wide Collaboration Services Objectives

~~*4.5.2.2 UC Network-Wide Collaboration Services Capability Increments*~~

Figure 4.4~~5~~.2-2, UC Pilot Increments, shows the near-term, mid-term, and long-term network-wide collaboration services capability increments. The initial increment moves forward with the testing of COTS UC solutions that are not capable of individually "class marking" IP packets consistent with the DSCP Plan shown in Section 5.3.3.3, General Network Requirements. Next, is the implementation and assessment of products that can mark individual flows (i.e., voice, video, IM/Chat) as belonging to a particular traffic class per UCR 2010, Differentiated Serviced ("DiffServ") requirements. Longer term, path is mapped for how these UC applications can migrate to assured services to better support the needs of the mission-critical users.

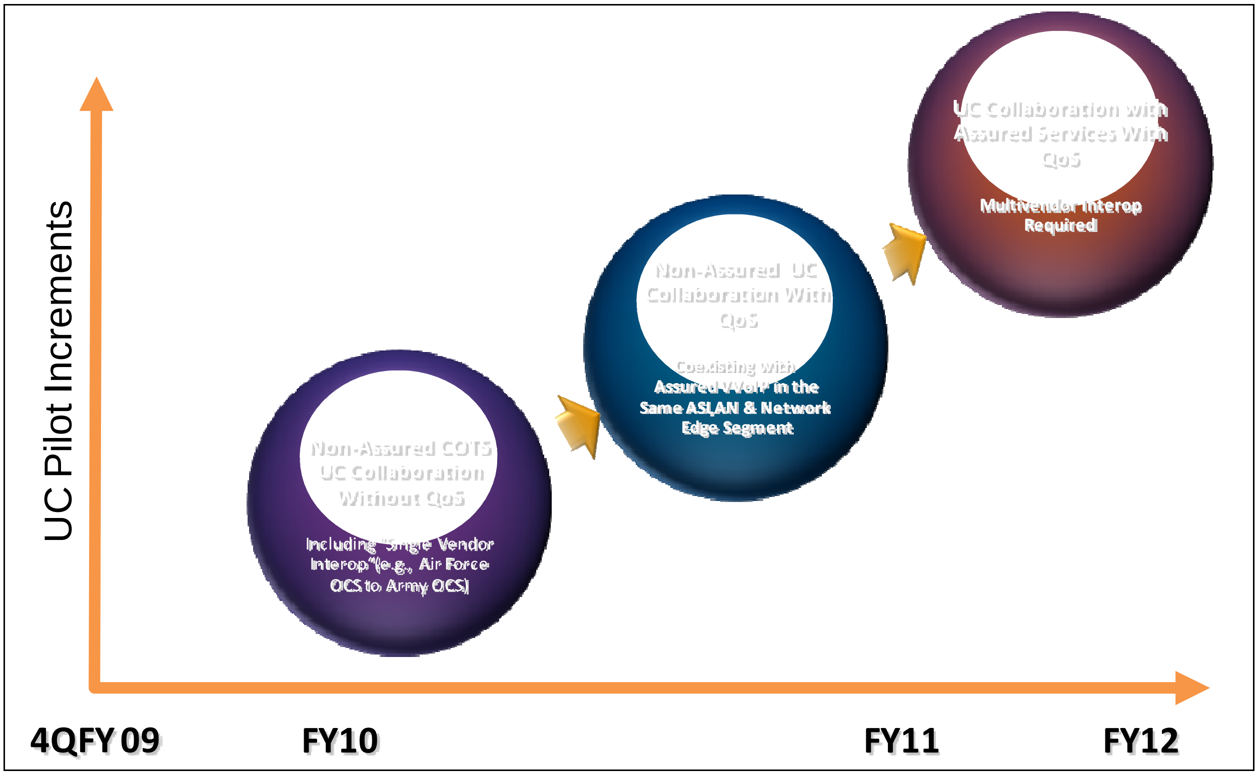

UC Pilot Increments
Non-Assured COTS UC Collaboration Without QoS
Including "Single Vendor Interop"(e.g., Air Force OCS to Army OCS)
Non-Assured UC Collaboration With QoS
Coexisting with Assured VVoIP in the Same ASLAN & Network Edge Segment
UC Collaboration with Assured Services With QoS
Multivendor Interop Required
4QFY 09
FY10
FY11
FY12

Figure 4.4~~5~~.2-2. UC Pilot Increments

~~*4.5.2.3 UC Network-wide Collaboration Services Capability Interoperability*~~

Multivendor interoperability is needed to exploit the full potential of IM, Chat, and Presence across the DoD. Without multisystem, multivendor interoperability/federation, users can only exchange Presence information and IMs with users who belong to the same system or the same COI. With multisystem, multivendor interoperability, the DoD community can exploit the full potential of IM, Chat, and Presence. The concept of Federating simply refers to a server-to-server link that permits the exchange of Presence information and IM between the two systems.

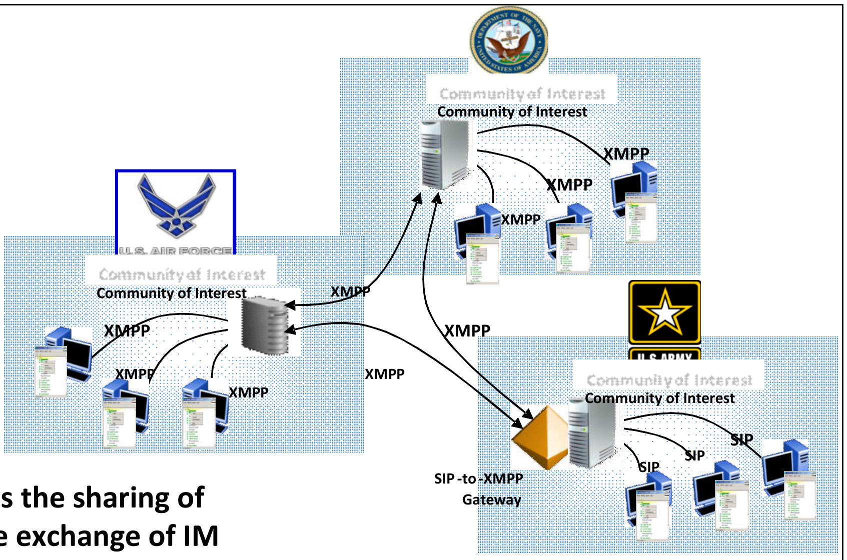
Figure 4.4~~5~~.2-3, Interoperability/Federation of IM, Chat, and Presence, illustrates the following IM, Chat, and Presence demonstrations:

- "Single vendor" interoperability (e.g., the ability to federate or bridge a vendor solution owned by the Air Force with the same vendor solution owned by another MILDEP)

- Multivendor interoperability

Demonstrate that the interoperability of IM/Chat and Presence can be achieved:

- **Within single vendor solutions.**
- **Within multivendor solutions.**
- **Using SIP-to-XMPP Gateways.**



- **Federation/Bridging involves the sharing of Presence information and the exchange of IM across multiple systems.**

- **Federation enables connectivity between otherwise isolated implementations allowing users who reside in different Communities of Interest (COIs) to exchange IM/Chat/Presence using open, standards-based protocols and UCR 2010 specifications.**

Figure 4.4~~5~~.2-3. Interoperability/Federation of IM, Chat, and Presence

- The ability to federate native Extensible Messaging and Presence Protocol (XMPP) IM clients with native SIP/SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) IM clients through a SIP-to-XMPP gateway

4.4~~5~~.2.2~~3~~ ~~Service Portability~~Integration of Voice, Video and Data Focused on Mobility

4.4.2.2.1 Service Portability

Service portability is defined as the end user’s ability to obtain subscribed services in a transparent manner regardless of the end user’s point of attachment to the network. The key UC objective is to provide service continuity by ensuring mobile warfighters’ telephone numbers, e-mail addresses, and communication and collaboration tools remain constant as their mission and location change. Figure 4.4~~5~~.~~3~~2-~~1~~4, Mobile Warfighter’s Communication Dilemma, shows the problem service portability is trying to solve.

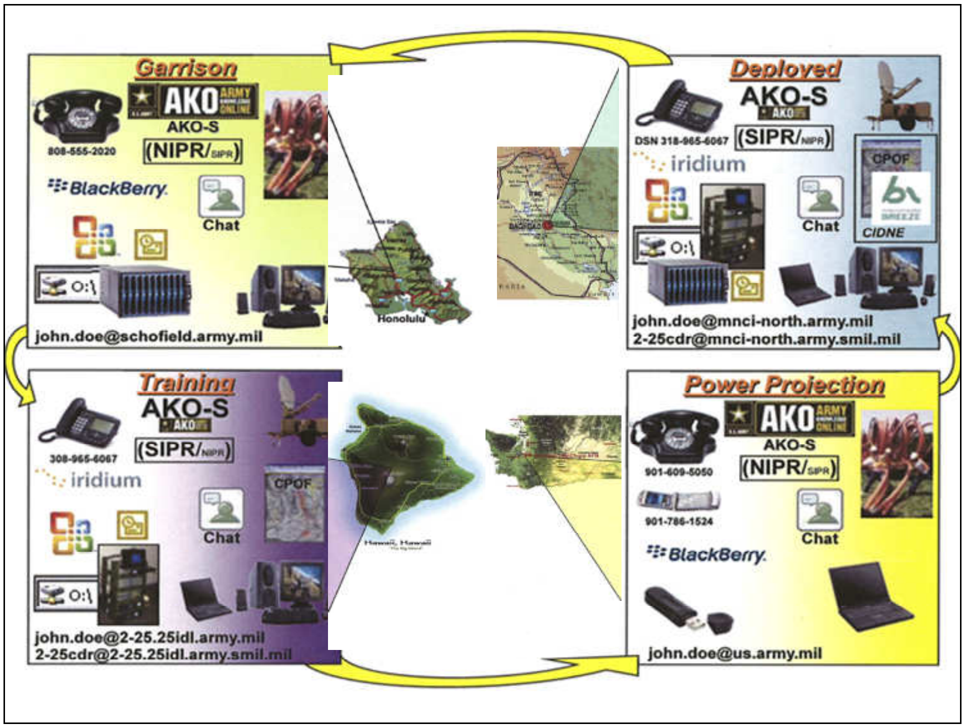


Figure 4.4~~5~~.~~3~~2-~~1~~4. Mobile Warfighter's Communication Dilemma

To achieve this objective, the UC architecture needs to address the issues of service discovery, centralized authentication and authorization, and centralized directory integration and access. Service discovery is focused on allowing a roaming end user's client to discover the location of the service (i.e., LSC, e-mail server, XMPP server). Centralized authentication and authorization permits roaming users to access the network and receive their assigned privileges. Centralized directory integration and access is associated with ensuring a roaming user has access to end-user lookups (i.e., white pages) and to enable automatic user provisioning.

The near-term strategy is to deploy and assess prototype solutions in Spiral 1 and work with sponsoring MILDEPs to define test objectives, user requirements, and to resolve Information Assurance issues in order to complete a architecture. The lessons learned during Spiral 1 will be used to attain the mid-term strategy to incorporate the architecture and requirements into the UCR 2010. Based on the vendors implementing the architecture and requirements within their products and systems, the long-term strategy is to test and field the products and systems within the Deployed and S environments in the 2012–2013 timeframe.

4.4.2.2.2 Multi~~Media~~Function Mobile Devices ~~(New Category)~~

Multifunction Mobile Devices is a new product category that will include products such as Smart Phones including SME PEDs. ~~and Smart Phone high level – See John Rutledge and Sam for material. Why isn't SME PED not the same as a Smart Phone?~~This product category will primarily consist of COTS products with added Information Assurance requirements.
In the context of this document, a "Smartphone End Instruement" is defined as an application that provides End Instrument (EI) or AS-SIP End Instrument (AEI) functions. However, unlike a traditional EI, this is an application that operates within the confines of an advanced, mobile computing platform (e.g. a smartphone, PDA, wireless tablet, etc.) which provides functionality beyond just basic telephony services. Figure 4.4.2-5 illustrates the relationship between a Smartphone EI and its operating platform.

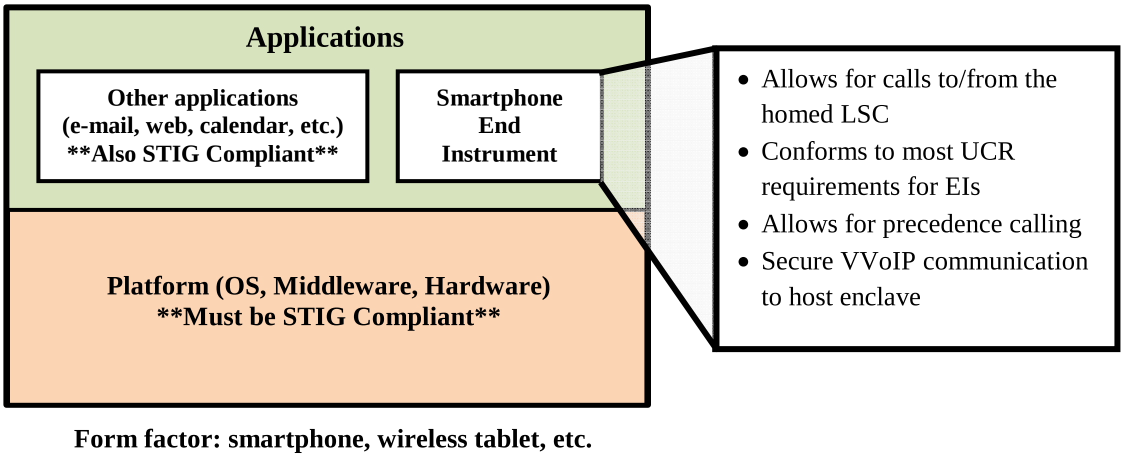

Applications
Other applications
(e-mail, web, calendar, etc.)
Also STIG Compliant
Smartphone
End
Instrument
Platform (OS, Middleware, Hardware)
Must be STIG Compliant
Allows for calls to/from the homed LSC
Conforms to most UCR requirements for EIs
Allows for precedence calling
Secure VVoIP communication to host enclave
Form factor: smartphone, wireless tablet, etc.

Figure 4.4.2-5: Smartphone End Instrument Relationship to the Host Platform

Even though a Smartphone End Instrument provides functionality similar to a standard End Instrument or AS-SIP end instrument, there are some important differences. First and perhaps most important, a Smartphone EI will typically operate over non-DoD controlled, public access networks to include the public Internet and wireless commercial carrier networks. Also, because public networks in many cases do not provide quality of service and availability guarantees, calls made using a Smartphone EI will not have availability comparable to calls originating from within the VVoIP enclave—in spite of the fact that an assured services VVoIP network is used within the enclave. Lastly, other applications operating on the same platform as the Smartphone EI could provide any number of e-mail, GPS, Bluetooth, web browsing, instant messaging, or SMS services. These additional services must not weaken the security posture of the device when it connects to the assured services VVoIP network.

The addition of Smartphone EIs to the VVoIP operating environment provides the opportunity for enhanced mobility and connectivty, but also requires the implementation of additional safeguards in order to maintain the security posture of the network. Unlike an EI or AEI, which has nearly direct network layer 3 connectivity to its homed LSC[1], a Smartphone EI is only permited to connect to its homed LSC in one of two ways:

1.) Establish an encrypted VVoIP signaling and media traffic session with a "Back-to-Back User Agent," providing functionality similar to an EBC, at the edge of the homed enclave. This Back-to-Back User Agent communicates on behalf of the Smartphone EI to the homed LSC using the LSC's native, vendor-defined line-side protocol or AS-SIP.

2.) Establish a VPN tunnel to a VPN Server located within the home enclave's DMZ. The VPN server extracts the VVoIP signaling from the VPN tunnel and transmits the information, to the homed LSC. If necessary, a translation step can occur at the VPN server if the information received/transmitted via the VPN tunnel is not already compatible with the LSC's vendor defined line-side protocol or AS-SIP.

4.4.3- Hybrid Networks Design for UC

~~{Jo~~During the transition period when TDM is being replaced IP-based UC, calls must be routed in
a hybrid network environment involving both the operational DSN and the evolving IP-based Assured Services network.

The following three objectives for hybrid network operation have been defined:

1. At the Base/Post/Camp/Station level, full Directory number portability is required as users transfer from a TDM-based End Office to an IP-based edge solution within a local serving area.

2. At the network (backbone) level, the quantity of E2E IP to TDM to IP conversion for calls shall be held to a minimum.

3. At the network (backbone) level, calls originating as IP shall remain IP as far as possible towards the terminating end; calls originating as TDM shall remain TDM as far as possible towards the terminating end.

The three rules defined above can be met by either employing a network-level 10-digit directory number based routing database, (the RTS Routing database described in Section 4.4.3.1) or by a careful coordination of the DSN numbering plan assignments and the standard six-digit DSN translation/routing tables.

[1] Though the term LSC is mainly used in this section, an SS or MFSS could also provide the same functionality for a Smartphone EI.

The network-level 10-digit directory number routing database that will associate a 10-digit directory number with the 'technology type' of the called end instrument (e.g., IP or TDM instrument) and direct routing accordingly down to the specific switching system (EO or LSC) serving the individual end instrument.

4.4.3.1 RTS Routing Database.

The RTS Routing Database is a DISA-owned and operated database that contains records of the DSN numbers, commercial (PSTN) numbers, LSC identifiers, and WAN SS / MFSS identifiers for RTS end users served by RTS LSCs. This database may also contain records of DSN numbers and commercial numbers for individual DSN end users served by DSN EOs and PBXes. The database records may be populated automatically by RTS LSCs, whenever an end user's numbers are added to an LSC during that activation of that end user on the LSC. The database records may also be populated manually by a DISA craftsperson, using DSN and commercial number information from an RTS LSC site or DSN EO/PBX site.

RTS LSCs that support the Commercial Cost Avoidance (CCA) feature query the RTS Routing DB to determine if there is a DSN number stored there that matches the dialed commercial number on a commercial call from the LSC (e.g., a 9+9 call, or a 9+8 call). WAN SSs and MFSSs that support the Hybrid Routing (HR) feature query the RTS Routing DB to determine if there is an LSC identifier, a Primary WAN SS/MFSS identifier, and a Backup WAN SS/MFSS identifier stored there that match the dialed DSN number on an RTS call that enters the WAN SS or MFSS.

The protocol that LSCs, MFSSes, and WAN SSes use to query and update the RTS Routing Database is Lightweight Directory Access Protocol Version 3 (LDAP v3), secured using Transport Layer Securty (TLS), and signaled via IP over the DISN WAN. In general, the RTS Routing DB is located at a centralized DISA site that is physically separate from the LSC site, the MFSS site, or the WAN SS site.
~~Add RTS Routing DB}~~

4.5~~6~~ UC PRODUCTS, APL PROCESSES, AND CONNECTION PROCESSES

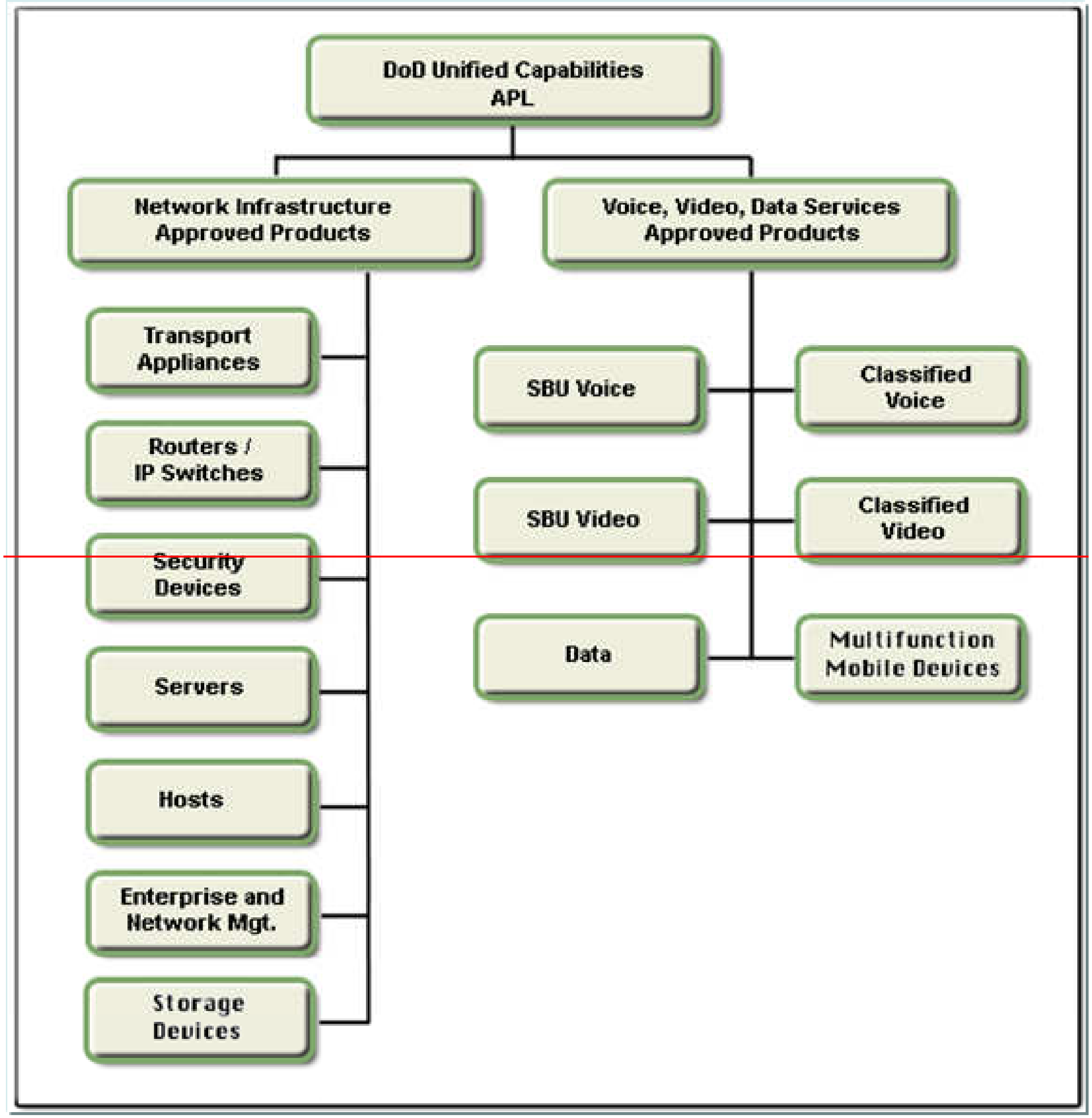
This section provides an overview of the APL product categories and products with those categories. It defines the processes used to get the products placed on the APL and processes needed to gain connection approvals for the products. More detailed information is available at http://www.disa.mil/ucco/.

4.5~~6~~.1 Overview of Approved Products

The UCR covers a broad variety of product categories and products within those categories that support UC. The two major product categories are network infrastructure and voice, video, and data services consistent with the definition of UC. Not all IT products are required to be on the APL. The DoD UC Steering Group advises ASD(NII)/DoD CIO with respect to which product categories and products should appear in the UCR, and thus, on the APL. APL products identified by the ASD(NII)/DoD CIO must be on the APL for DoD Components to acquire them. Products that have not been identified by the ASD(NII)/DoD CIO to be on the APL can be acquired by DoD Components. Still products must be granted a site Authority to Operate (ATO) and be operated IAW appropriate STIGs to gain DISN Authority to Connect (ATC).

Figure 4.5.1-1, Overview of UC Product Categories within the DoD UC APL, provides an overview of the structure of the DoD UC APL in terms of services and network infrastructure. The various UC products for each UC product category would be found under their appropriate section of the UC APL. Many UC products would show up under multiple UC product categories since they can be used under multiple categories. Examples include the LSCs, CE Routers, EBCs, and ASLANs that can be used for both SBU and Classified voice and video services.

The term appliance or appliance functions are used throughout the UCR as a generic term referring to a function or feature which may be part of a UC APL product.


DoD Unified Capabilities APL
Network Infrastructure Approved Products
Voice, Video, Data Services Approved Products
Transport Appliances
Routers / IP Switches
Security Devices
Servers
Hosts
Enterprise and Network Mgt.
Storage Devices
SBU Voice
Classified Voice
SBU Video
Classified Video
Data
Multifunction Mobile Devices

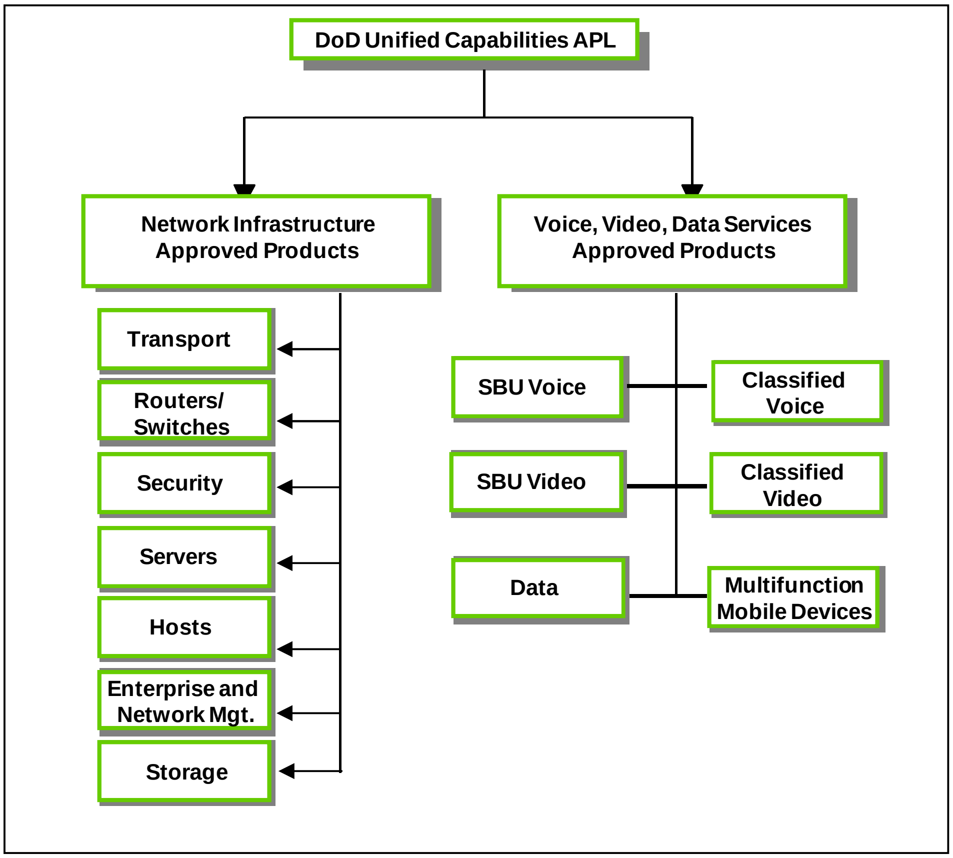

DoD Unified Capabilities APL
Network Infrastructure Approved Products
Voice, Video, Data Services Approved Products
Transport
Routers/ Switches
Security
Servers
Hosts
Enterprise and Network Mgt.
Storage
SBU Voice
Classified Voice
SBU Video
Classified Video
Data
Multifunction Mobile Devices

Figure 4.5.1-1. Overview of UC Product Categories within the DoD UC APL

~~Figure 4.5.1-1, Overview of UC Product Categories within the DoD UC APL, provides an overview of the structure of the DoD UC APL in terms of services and network infrastructure. The various UC products for each of the six UC product categories would be found under their appropriate section of the UC APL. Many UC products would show up under multiple UC product categories since they can be used under multiple categories. Examples include the LSCs, CE Routers, EBCs, and ASLANs that can be used for both SBU and Classified voice and video services.~~

~~{Build a better explanation of the relationship between the categories and the product types within each category. Introduce product types for the Figure 4.6.1-1 and -2.}~~

4.5.1.1 Network Infrastructure Approved Products

Table 4.5.1-2 through Table 4.5.1-6 ~~T~~within this section list~~s~~ the products for the following Network Infrastructure Approved Products categories:

- Transport ~~Appliances~~
- Routers / ~~IP~~ Switches
- Security ~~Devices~~
- Enterprise and Network Management
- Storage ~~Devices~~
- Hosts*
- Servers*

* There are currently no UC products that the UC Steering Group has approved for inclusion in the Host and Server Categories.
-Currently, Data-At-Rest products, Personal Information Integrity (PII)/Data Leakage and HAIPE discovery servers are being assessed for applicability for inclusion with UCR

Table 4.5.1-~~1~~2 Transport Appliances

Product	**Requirements Section**	**Role and Function**
Access Grooming Functional (AGF) Device	5.5	Product that receives low-speed circuits on multiple ports and multiplexes them via TDM into a high-speed circuit, and transmits it to one of its high-speed ports.
~~MSPP~~Access Aggregation Function M13 Device	5.5	~~Product providing access to the DISN WAN from the Edge by multiplexing lower bandwidth connections to higher speed circuits~~Product that functionally multiplexes DS1s into a DS3
Optical Transport System (OTS)	5.5	Switching product providing high-speed optical transport in the DISN WAN
Fixed network Element	5.9	Product that provides transport for bearer and signaling traffic in a fixed network environment.
Deployed network Element	5.9	Product that provides transport for bearer and signaling traffic in a deployed network environment

Table 4.5.1-~~2~~3 Router/~~IP~~ Switches

Product	**Requirements Section**	**Role and Function**
Aggregation Router	5.5	Product serving as a port expander for a PE Router

Provider Edge Router	5.5	Product providing robust, high-capacity IP routing at the entry points to the DISN WAN
Provider Router	5.5	Product providing robust, high-capacity IP routing in the DISN WAN
Customer Edge Router	5.3.2	Product providing IP routing towards the DISN WAN at a customer edge
Access IP Switch	5.3.1	Product used in a LAN to provide end-device access to the LAN
Distribution IP Switch	5.3.1	Product used in a LAN to provide intermediate switching layer between a LAN access and core layers
Core IP Switch	5.3.1	Product providing high speed IP switching at the LAN core layer
Wireless LAN Equipment	5.3.1	Products used in Wireless LANs: Wireless End Instrument, Wireless LAN Access System, Wireless Access bridges

~~Currently, Data-At-Rest products, Personal Information Integrity (PII)/Data Leakage and HAIPE discovery servers are being assessed for applicability for inclusion with UCR~~

Table 4.5.1-~~3~~4 Security Devices

Product	**Requirements Section**	**Role and Function**
EBC	5.3.2, 5.3.4, 5.3.5, 5.4	A product that provides firewall functions for voice traffic (Also Listed under Voice products)
Data Firewall	5.8	A product that blocks unauthorized access while permitting authorized communications.
VPN Concentrator	5.8	A product that sets up a secure link between an end user and an internal network.
Intrusion Protection System (IPS)	5.8	A product that detects unwanted attempts at accessing, manipulating, and/or disabling a computer system.
HAIPE	5.6 ~~(should be latency that we can tolerate for Voice and Video)~~	HAIPE is a programmable IP INFOSEC device with traffic protection, networking, and management features

		that provide Information Assurance services for IPv4 and IPv6 networks. Encryption algorithms are not specified and are under the authority of NSA.
Link Encryptors	5.6 ~~(should include latency that Voice and Video can tolerate)~~	Link Encryptors provide data security in a multitude of NEs, by encrypting point-to-point, netted, broadcast, or high-speed trunks. Encryption algorithms are not specified and are under the authority of NSA.
Integrated Security Solution	5.8	A product that provides the functionality of more than one IA device in one integrated device
IA Tools	5.8	Products that provide Information Assurance functions
Network Access Control	5.8	Products that provide Information Assurance functions

LEGEND			
HAIPE	High Assurance Internet Protocol Encryptor	IPv4	Internet Protocol Version 4
FW	Firewall	IPv6	Internet Protocol Version 6
INFOSEC	Information Security	NSA	National Security Agency
IPS	Intrusion Protection System	VPN	Virtual Private Network

Table 4.5.1-~~4~~5 Enterprise and Network Management

Product	**Requirements Section**	**Role and Function**
Element Management System	~~5.11~~5.11	For monitoring FCAPS and command elements (products operating in a network).
Operational Support Systems	5.11	Manager of element managers for FCAPS and for information sharing.

Table 4.5.1-~~5~~6 Storage ~~Devices~~

Product	**Requirements Section**	**Role and Function**
Data Storage Controller	5.10.~~X~~	Specialized multi-protocol computer system with an attached disk array that together serves in the role of a disk array controller and end-node in B/P/C/S networks.

4.5.1.2 Voice, Video, Data Services Approved Products

Table 4.5.~~1~~2-~~6~~1 lists the products in SBU UC Voice Product Category.

Table 4.5.~~1~~2-~~6~~1 SBU Voice

Product	**Requirements Section**	**Role and Function**
Local Session Controller	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Product that provides many local telephony (UC) functions
MFSS	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Large, complex product that provides many local and WAN-related telephony functions
WAN SS	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	A product that acts as an AS-SIP B2BUA within the UC architecture. It provides the equivalent functionality of a commercial SS and has similar functionality to the SS component of an MFSS
AS-SIP End Instruments		End instrument using AS-SIP signaling
'RTS' Routing Database	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Product that provides Cost Avoidance Routing and Hybrid Call Routing Translations at the network-level
EBC	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	A product that provides firewall functions for voice traffic (Also Listed under Security products)
AS-SIP to TDM Gateway	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Product that provides interworking between AS-SIP, IP bearer and TDM signaling and bearer
AS-SIP to IP Gateway	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Product that provides interworking between AS-SIP and proprietary UC appliance signaling
RTS Stateful Firewall (RSF)	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Product that acts as a Firewall protecting an LSC or SS
Multi-Signaling Conference Bridge	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Product that provides conferencing capabilities where endpoints use different signaling protocols

Table 4.5.~~1~~2-~~7~~2 lists the products in Classified UC Voice Product Category.

Table 4.5.~~1~~2-~~7~~2 Classified Voice

Product	**Requirements Section**	**Role and Function**
Local Session Controller	5.3.2 (AS Features), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA), 6.2 Classified	Same as SBU Voice
Dual Signaling Softswitch	5.3.2 (AS Features), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA), 6.2 Classified	Unique to Classified
AS-SIP End Instruments	5.3.2 (AS Features), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA), 6.2 Classified	Unique to Classified

Table 4.5.~~1~~2-~~8~~3 lists the products in SBU UC Video Product Category.

Table 4.5.~~1~~2-~~8~~3 SBU Video

Product	**Requirements Section**	**Role and Function**
Local Session Controller	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Same product as voice LSC.
MFSS	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Same product as voice MFSS.
WAN SS	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Same product as voice WAN SS
AS-SIP End Instruments	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Unique to video…
Multi Signaling MCU	5.3.2 (AS Req), 5.3.4 (AS-SIP), 5.3.5 (IPv6), 5.4 (IA)	Unique to video….

Table 4.5.~~1~~2-~~9~~4 lists the products in Classified UC Video Product Category.

Table 4.5.~~1~~2-~~9~~4 Classified Video

Product	**Requirements Section**	**Role and Function**
Local Session Controller	6.2	Same product as voice LSC.
Dual Signaling Softswitch	6.2	Unique to Classified
AS-SIP End Instruments	6.2	Unique to video and Classified
Multi Signaling MCU	6.2	Unique to video

4.5.1.3 Data Category Approved Products

Data category products can include various combinations of the following data applications:

- E-mail/calendaring
- Unified messaging
- Web conferencing and web collaboration
- Unified conferencing
- Instant messaging and chat
- Rich presence

These data applications are features of UC Tool Suites and are considered to be data UC products. In addition, these data applications can be network aware in order to get enhanced quality of service treatment on DoD networks. In those cases, the interface is specified for interoperability but the performance (e.g., response time, screen refresh rate) of the applications are not currently specified. These UC Tool Suites can be integrated with voice and video services in order to get assured services as well as QoS. Examples would be LSCs that include voice, video and XMPP functionality as well as unified messaging. Table 4.5.~~1~~3-~~10~~1 lists the data category products.

Table 4.5.~~1~~3-1~~10~~ Data Category Products

Product	**Requirements Section**	**Role and Function**
UC Tool Suite with specific features identified (XMPP Server, XMPP Client)	5.7	Integrated voice, video and data services that operate at various security levels over a hand held device with wireless secure connectivity to the network or a desktop device with secure connectivity to the network.

4.5.1.4 Multifunction Mobile Devices Products

A multifunction mobile device, or, "Smartphone End Instrument" is defined as an application that provides End Instrument (EI) or AS-SIP End Instrument (AEI) functions. However, unlike a traditional EI, this is an application that operates within the confines of an advanced, mobile computing platform (e.g. a smartphone, PDA, wireless tablet, etc.) which provides functionality beyond just basic telephony services. Security requirements, rather than functional requirements are specified for these devices.

Table 4.5.~~1~~4-~~11~~1 Multifunction Mobile Devices

Product	**Requirements Section**	**Role and Function**
Classified Multi Media Device	5.4	Integrated voice, video and data services that operate at multiple security levels over a hand held device with wireless secure connectivity to the network (pull definition from #10) e.g., SME PED, smartphones
SBU Multi Media Device	5.4	Integrated voice, video and data services that operate at an SBU security level only over a hand held device with wireless secure connectivity to the network (e.g., SME PED, smartphones)

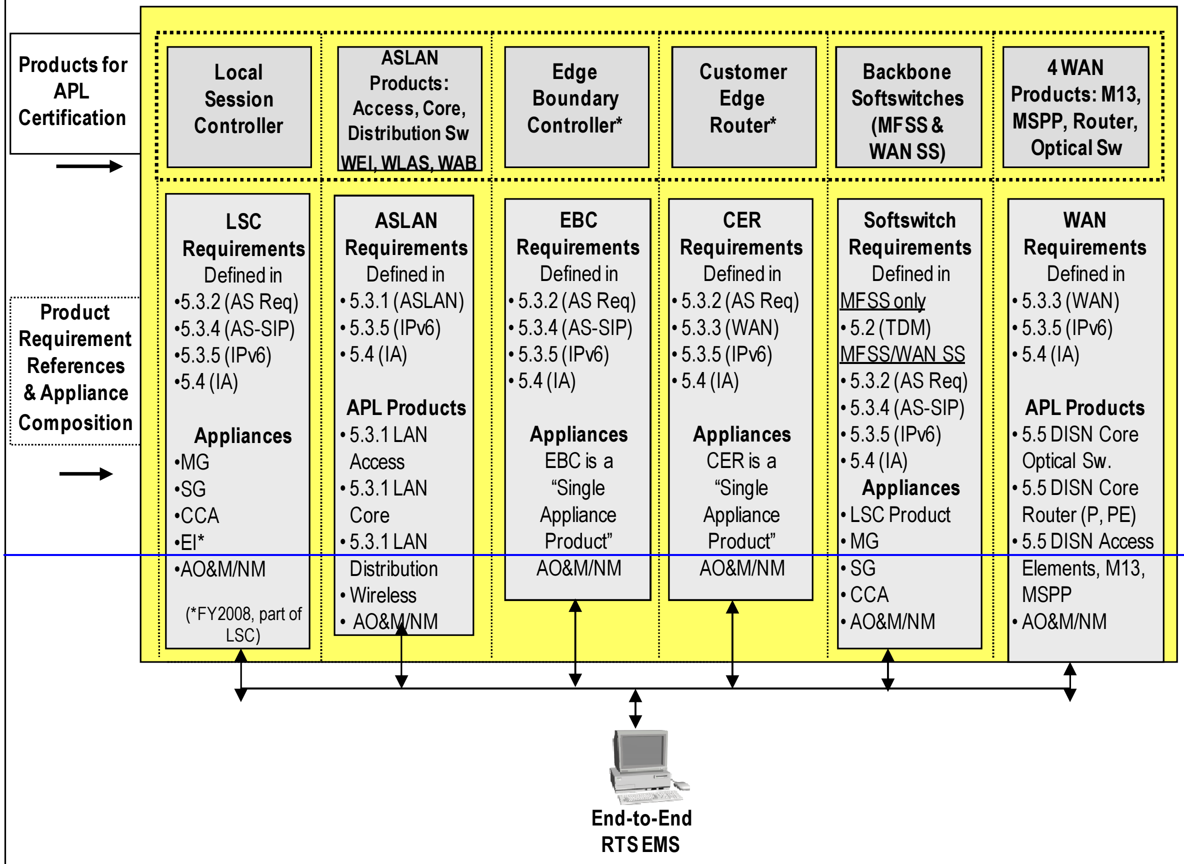
4.5.1.5 Deployable UC Products

~~Instant Messaging, Chat, Presence, and Collaboration UC Tool Suites are considered to be data UC products. These applications create the possibility of real-time, text-based communication between two or more participants over the network infrastructure. These UC features are included in the SBU UC products for IP E2E systems that support SBU voice and video services; classified UC products for IP E2E systems that support SBU voice and video services; and in deployable products.~~

~~Figure 4.6.1-1, SBU UC Product Categories for IP E2E Systems that Support IP-Based SBU Voice and Video Services, delineates the SBU UC products for IP E2E systems that support SBU voice and video services.~~

~~Figure 4.6.1-2, Classified VoIP UC Products, delineates the classified UC products.~~

Illustration of IP-based UC products to be tested for APL certification with high-level reference to UCR 2008 requirements sections. Products consists of one or several appliances. NOTE: Figure does not illustrate physical packaging of products and their appliances.

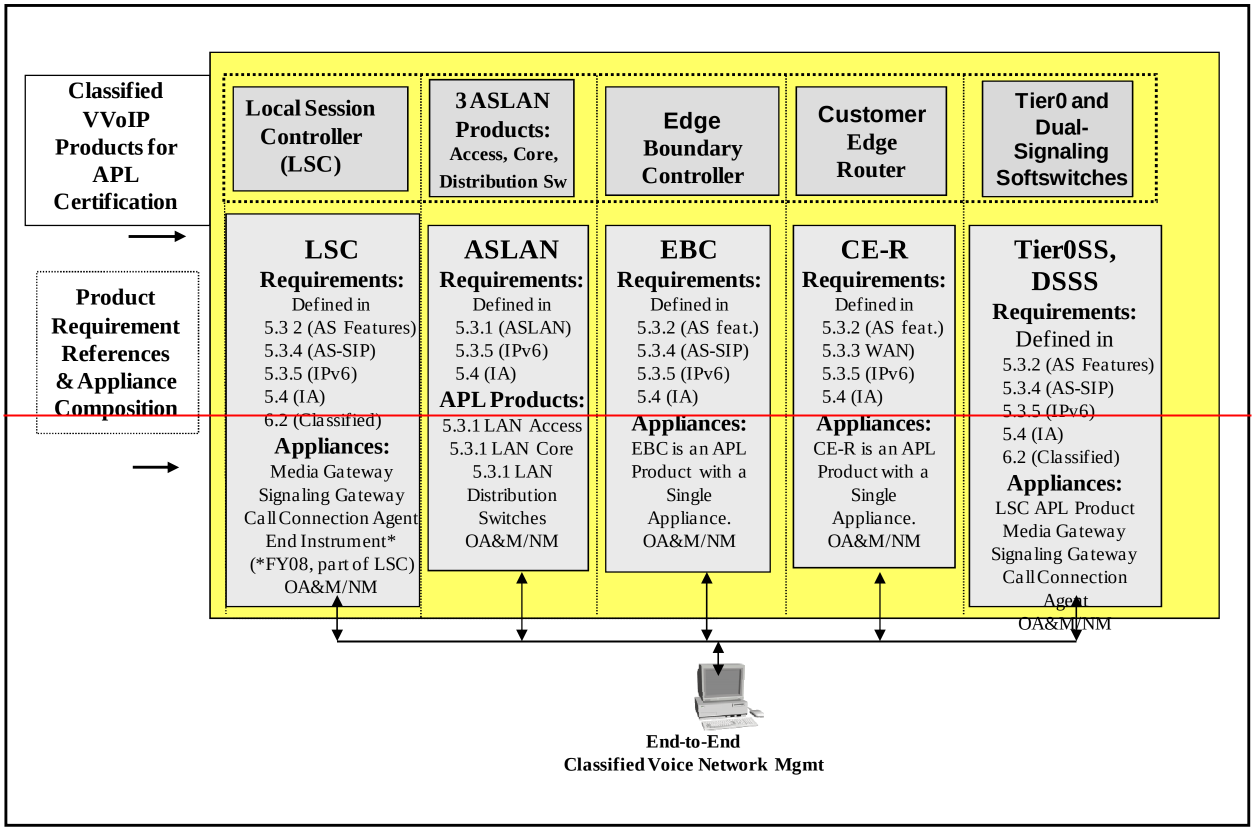


AS Req (described in UCR 2008, Section 5.3.2) is not an APL product, Assured Services are provided by call control with MUFs using functions and features from the ten APL products and AS-SIP signaling.

LEGEND

ADIMSS	Advanced DSN Integrated Management Support System	EI	End Instrument	MSPP	Multi-Service Provisioning Platforms
		FY	Fiscal Year	MUF	Military Unique Features
AO&M	Administration, Operations, and Maintenance	IA	Information Assurance	NM	Network Management
APL	Approved Products List	INMS	Integrated Network Management System	P	Provider
ARTS	Assured Real Time Services	IP	Internet Protocol	PE	Provider Edge
ASLAN	Assured Services Local Area Network	IPv6	Internet Protocol Version 6	RTS	Real Time Services
AS-SIP	Assured Services Session Initiation Protocol	LAN	Local Area Network	SG	Signaling Gateway
CCA	Call Connection Agent	LSC	Local Session Controller	Sw	Switch
CER	Customer Edge Router	MFSS	Multifunction Softswitch	UCR	Unified Capabilities Requirements
DISN	Defense Information Systems Network	MG	Media Gateway	WAN	Wide Area Network
EBC	Edge Boundary Controller				

~~**Figure 4.6.1-1. SBU UC Product Categories for IP E2E Systems that Support IP-Based SBU Voice and Video Services**~~


Classified VVoIP Products for APL Certification
Product Requirement References & Appliance Composition
Local Session Controller (LSC)
3 ASLAN Products: Access, Core, Distribution Sw
Edge Boundary Controller
Customer Edge Router
Tier0 and Dual-Signaling Softswitches
LSC Requirements: Defined in 5.3 2 (AS Features) 5.3.4 (AS-SIP) 5.3.5 (IPv6) 5.4 (IA) 6.2 (Classified)
Appliances: Media Gateway Signaling Gateway Call Connection Agent End Instrument* (*FY08, part of LSC) OA&M/NM
ASLAN Requirements: Defined in 5.3.1 (ASLAN) 5.3.5 (IPv6) 5.4 (IA)
APL Products: 5.3.1 LAN Access 5.3.1 LAN Core 5.3.1 LAN Distribution Switches OA&M/NM
EBC Requirements: Defined in 5.3.2 (AS feat.) 5.3.4 (AS-SIP) 5.3.5 (IPv6) 5.4 (IA)
Appliances: EBC is an APL Product with a Single Appliance. OA&M/NM
CE-R Requirements: Defined in 5.3.2 (AS feat.) 5.3.3 WAN) 5.3.5 (IPv6) 5.4 (IA)
Appliances: CE-R is an APL Product with a Single Appliance. OA&M/NM
Tier0SS, DSSS Requirements: Defined in 5.3.2 (AS Features) 5.3.4 (AS-SIP) 5.3.5 (IPv6) 5.4 (IA) 6.2 (Classified)
Appliances: LSC APL Product Media Gateway Signaling Gateway Call Connection Agent OA&M/NM
End-to-End Classified Voice Network Mgmt

~~**Figure 4.6.1-2. Classified VoIP UC Products**~~

~~Table 4.6.1-1, DISN Network Infrastructure UC Product Categories, delineates the network infrastructure UC products that can be used by all MILDEPs for their Intranets. These UC products do not currently include data firewalls but will in future updates.~~

~~Table 4.6.1-1. DISN Network Infrastructure UC Product Categories~~

~~Item~~	~~requirements section~~	~~Role and Functions~~
~~M13~~	~~5.5~~	~~Product providing access to the DISN WAN from the Edge by multiplexing lower bandwidth connections to higher speed circuits~~
~~MSPP~~	~~5.5~~	~~Product providing access to the DISN WAN from the Edge by multiplexing lower bandwidth connections to higher speed circuits~~
~~Aggregation Router~~	~~5.5~~	~~Product serving as a port expander for a PE Router~~
~~Provider Edge Router~~	~~5.5~~	~~Product providing robust, high-capacity IP routing at the entry points to the DISN WAN~~
~~Provider Router~~	~~5.5~~	~~Product providing robust, high-capacity IP routing in the DISN WAN~~
~~Optical Switch~~	~~5.5~~	~~Switching product providing high-speed optical transport in the DISN WAN~~
~~LEGEND~~ ~~DISN Defense Information Systems Network~~ ~~IP Internet Protocol~~ ~~MSPP Multi-Service Provisioning Platforms~~		~~PE Provider Edge~~ ~~WAN Wide Area Network~~

Table 4.~~6~~5.~~1~~5-~~2~~1 delineates the deployable UC products. These products are based on configuring and installing UC products in a deployed environment. Table 4.5.5-1 does not list ‘Legacy’ deployable products which are found in UCR 2008.

Table 4.~~6~~5.~~1~~1-~~2~~5. Deployable UC Products ~~Categories~~ and Paragraph References

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
DVX-C	6.1.3	Deployable voice switch with ASF capabilities to support assured services requirements. This switch is used for rapid deployment situations and contingencies in the deployed environment.
Deployable NEs	5.9.3	NEs used in~~ a~~ deployed situations.
Deployable LANs	5.3.1 6.1.5	LAN used in deployed situations.
Deployed Tactical Radio	6.1.7	Deployable Radio systems used in~~ a~~ deployed situations.
DCVX	6.1.6	Deployable cellular voice switch with ASF capabilities to support assured services requirements. This switch is used for rapid deployment situations and contingencies.

LEGEND

ASF	Assured Services Features
DCVX	Deployed Cellular Voice Exchange
DVX-C	Deployable Voice Exchange – COTS
LAN	Local Area Network
NEs	Network Elements

~~Table 4.6.1-3 delineates the encryption products. All these UC products include IPv6 capability.~~

~~Table 4.6.1-3. Security Devices and Paragraph Reference~~

~~ITEM~~	~~REQUIREMENTS SECTION~~	~~ROLE AND FUNCTIONS~~
~~HAIPE~~	~~5.6~~	~~HAIPE is a programmable IP INFOSEC device with traffic protection, networking, and management features that provide Information Assurance services for IPv4 and IPv6 networks. Encryption algorithms are not specified and are under the authority of NSA.~~
~~Link Encryptors~~	~~5.6~~	~~Link Encryptors provide data security in a multitude of NEs, by encrypting point-to-point, netted, broadcast, or high-speed trunks. Encryption algorithms are not specified and are under the authority of NSA.~~
~~FW~~	~~5.8~~	~~A product that blocks unauthorized access while permitting authorized communications.~~
~~IPS~~	~~5.8~~	~~A product that detects unwanted attempts at accessing, manipulating, and/or disabling a computer system.~~
~~VPN Concentrator~~	~~5.8~~	~~A product that sets up a secure link between an end user and an internal network.~~

~~LEGEND~~

~~HAIPE~~	~~High Assurance Internet Protocol Encryptor~~
~~FW~~	~~Firewall~~
~~INFOSEC~~	~~Information Security~~
~~IPS~~	~~Intrusion Protection System~~
~~IPv4~~	~~Internet Protocol Version 4~~
~~IPv6~~	~~Internet Protocol Version 6~~
~~NSA~~	~~National Security Agency~~
~~VPN~~	~~Virtual Private Network~~

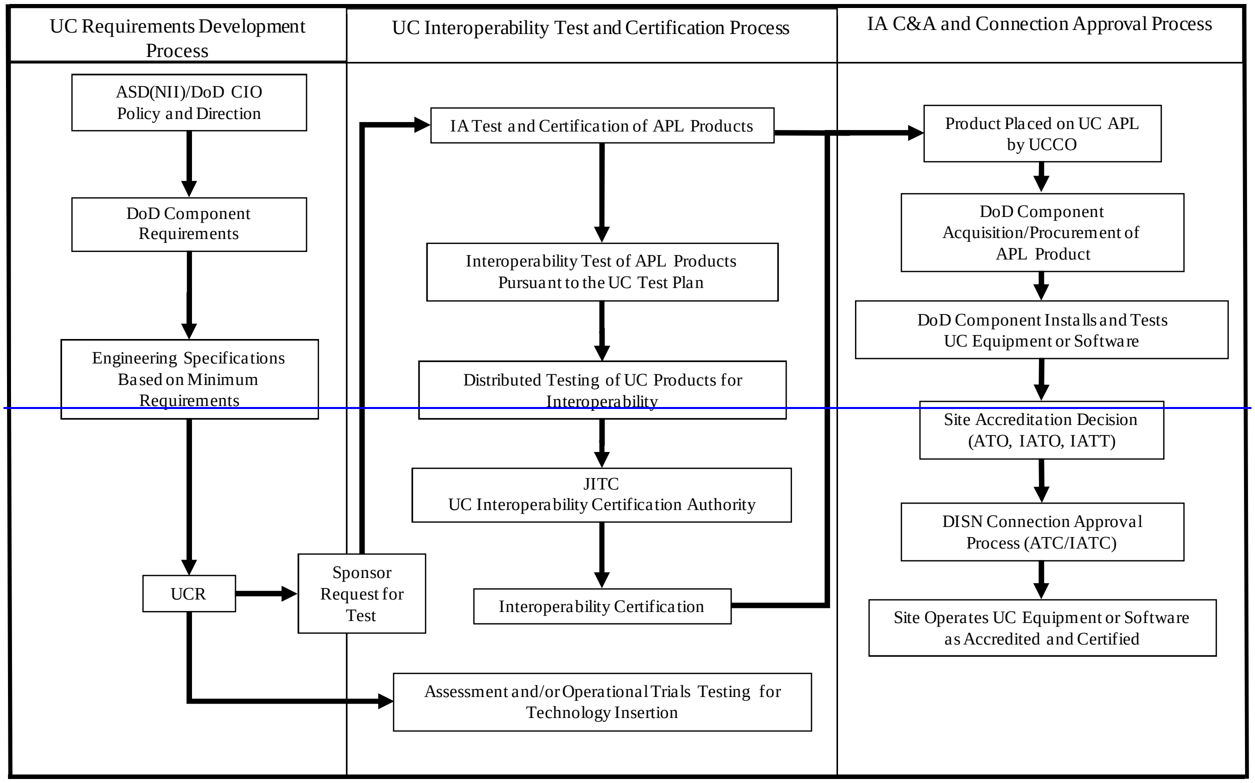
~~The UC products acquired by the DoD Components, and connected or planned for connection to DoD networks, shall be both Interoperability and Information Assurance certified by DISA pursuant to the current UCR.~~

4.5~~6~~.2 Overview of UC Interoperability and Information Assurance Processes

The UC Interoperability certification, IA certification and connection approval processes are illustrated in DoDI 8100.ee Enclosure 3 under the topic, "-UC C~~ertification~~ertification for Interoperability ~~AND~~and IA, and connection
— A~~PPROVA~~pproval~~L,~~ P~~ROCESSES~~rocesses

~~Figure 4.6.2-1, UC Requirements, Interoperability Certification, and Connection Approval Process. All UC products shall be tested and certified for Interoperability:~~

~~1. The ASD(NII)/DoD CIO provides overall policy and direction for development of UC requirements. DISA translates DoD Component functional requirements into engineering specifications for inclusion in the UCR. The ASD(NII)/DoD CIO approves the UCR for use in test and certification of UC products. The Joint Interoperability Test Command (JITC) develops the UC Test Plan (TP) based on the UCR. The UCR also may be used for UC product assessments and/or operational tests for emerging UC technology.~~

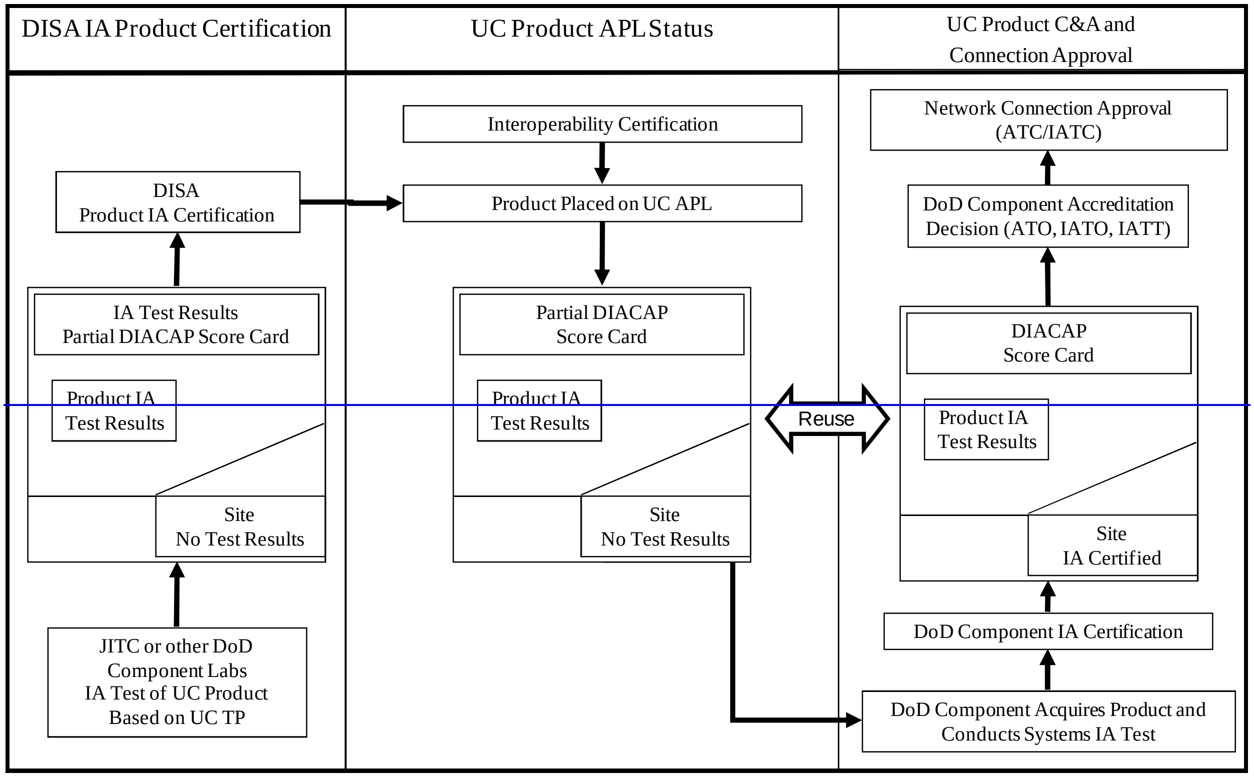

UC Requirements Development Process
UC Interoperability Test and Certification Process
IA C&A and Connection Approval Process
ASD(NII)/DoD CIO Policy and Direction
DoD Component Requirements
Engineering Specifications Based on Minimum Requirements
UCR
Sponsor Request for Test
IA Test and Certification of APL Products
Interoperability Test of APL Products Pursuant to the UC Test Plan
Distributed Testing of UC Products for Interoperability
JITC UC Interoperability Certification Authority
Interoperability Certification
Assessment and/or Operational Trials Testing for Technology Insertion
Product Placed on UC APL by UCCO
DoD Component Acquisition/Procurement of APL Product
DoD Component Installs and Tests UC Equipment or Software
Site Accreditation Decision (ATO, IATO, IATT)
DISN Connection Approval Process (ATC/IATC)
Site Operates UC Equipment or Software as Accredited and Certified

~~Figure 4.6.2-1. UC Requirements, Interoperability Certification, and Connection Approval Process~~

~~2. The JITC conducts Interoperability testing, adjudicates Interoperability test results, and provides certification, as appropriate. Figure 4.6.2-1, UC Requirements, Interoperability Certification, and Connection Approval Process, depicts an overview of the UC requirements, Interoperability certification, and connection approval processes. The JITC uses distributed testing for UC Interoperability certification. The JITC serves as the UC Interoperability certifying authority.~~

~~3. The UC products certified for both Interoperability and Information Assurance shall be placed on the DoD UC APL by the UCCO. This APL is the single authoritative source for certified UC products on DoD networks. The DoD Components are required to acquire or operate only UC products listed on the UC APL, unless and until a waiver is approved. The DoD Components provide a site accreditation decision for the UC product to be installed. This accreditation decision may result in an ATO, Interim Authorization to Operate (IATO), or Interim Authorization to Test (IATT). DISA then provides an ATC or Interim Approval to Connect (IATC) to the DISN. When installed and connected, UC products shall be operated and maintained pursuant to DISA STIGs and the JITC Interoperability certified configuration.~~

~~The UC Information assurance certification, accreditation, and connection approval processes are illustrated in Figure 4.6.2-2, UC Information Assurance Certification and Accreditation Process. The UC products on the DoD UC APL shall be granted Information Assurance certification by the DISA Certification Authority (CA).~~


DISA IA Product Certification
UC Product APL Status
UC Product C&A and Connection Approval
Interoperability Certification
Product Placed on UC APL
Network Connection Approval (ATC/IATC)
DoD Component Accreditation Decision (ATO, IATO, IATT)
DISA Product IA Certification
IA Test Results Partial DIACAP Score Card
Product IA Test Results
Site No Test Results
Partial DIACAP Score Card
Product IA Test Results
Site No Test Results
Reuse
DIACAP Score Card
Product IA Test Results
Site IA Certified
DoD Component IA Certification
DoD Component Acquires Product and Conducts Systems IA Test
JITC or other DoD Component Labs IA Test of UC Product Based on UC TP

~~Figure 4.6.2-2. UC Information Assurance Certification and Accreditation Process~~

~~DISA oversees the Information Assurance certification process for UC products. The DoD Component Designated Accrediting Authorities (DAAs) certifies and accredits information systems (ISs).~~

~~1. DISA and other DoD Component test labs conduct Information Assurance testing and adjudicate Information Assurance test results for security features of products that provide UC services. The DISA CA issues Information Assurance certification. Once a UC product has received both Interoperability and Information Assurance certifications, that product is placed on the APL. Figure 4.6.2-2 depicts the UC Information Assurance certification process.~~
~~2. The UC ISs are certified and accredited on a site-specific basis by the DoD Component DAA as part of the overall DoD Information Assurance Certification and Accreditation Process (DIACAP).~~
~~3. As an artifact of the Information Assurance test and certification process, the DoD Component test labs produce a partial DIACAP Score Card (as DoD Component test labs can completely test only a limited subset of Information Assurance controls, the remainder of the Information Assurance control tests must be completed on a site-specific basis, after Information Assurance certification). The partial DIACAP Score Card supports the Information Assurance certification and/or a type accreditation decision, and can assist a site in creating and~~

~~implementing a security baseline, providing the foundation for obtaining an ATO. DISA maintains a repository of partial DIACAP Score Cards for reuse by the DoD Components.~~

4.5~~6~~.3 Unified Capabilities Certification Office Processes

This section provides an overview of the UC approved products UCCO processes.
This process is defined for mature products and for technology insertion products that are evaluated via assessment testing in DoD test labs and validated for NETOPS via Spirals that deploy capabilities. Table 4.~~6~~5.3-1 provides a matrix framework for deciding the maturity of technologies and the mission criticality of the features provided by the technologies. This matrix is used to determine which technologies need technology insertion assessment testing and DISN UC Spiral Deployment validations (i.e., prototype and preproduction assured and affecting assured services) and which are ready for product approval testing (i.e., APL or post APL testing of assured or affecting assured services). If the features are non-assured and do not affect Assured services, there is no need to test them and a vendor letter of compliance (LOC) will be accepted. Two processes, APL processes for mature products and APL process for technology insertion products, are addressed in the subsequent sections.

Table 4.~~6~~5.3-1. Service Complexity vs. Technology Maturity Matrix for Determination of Type of APL Process

Services Complexity	Prototype	Pre-Production	APL Ready	Post APL
ASFs	• Full test • Or incremental test and/or desk-top review (DTR) if based on previously tested product	• Full test • Or incremental test and/or DTR if based on previously tested product	• Full test • Or incremental test and/or DTR if based on previously tested product	• Full test for new software versions or significant IA-affecting hardware changes • Or incremental test and/or DTR if based on previously tested product
Non ASFs Affecting ASFs	• Partial test • Full test of interaction of features • Or incremental test and/or DTR if based on previously tested product • No test. Vendor letter of compliance (LOC) of vendor tests of non assured services features meeting brochure claims	• Partial test • Full test of interaction of features • Or incremental test and/or DTR if based on previously tested product • No test. Vendor LOC of vendor tests of non ASFs meeting brochure claims	• Partial test • Full test of interaction of features • Or incremental test and/or DTR if based on previously tested product • No test. Vendor LOC of vendor tests of non ASFs meeting brochure claims	• Partial test • Full test of interaction of features for new software versions or significant IA-affecting hardware changes • Or incremental test and/or DTR if based on previously tested product • No test. Vendor LOC of vendor tests of non ASFs meeting brochure claims
Non ASFs Not Affecting ASFs	• Random test of potential interactions	• Random test of potential interactions	• No test • Vendor LOC of vendor tests of features meeting brochure claims	• No test • Vendor LOC of vendor tests of features meeting brochure claims

4.~~6~~5.3.1 Standard Process for Gaining APL Status

The standard process for gaining APL status for all UC products is shown in Figure 4.~~6~~5.3-1. This process reflects that both Interoperability and Information Assurance certifications are required for placement on the UC APL.

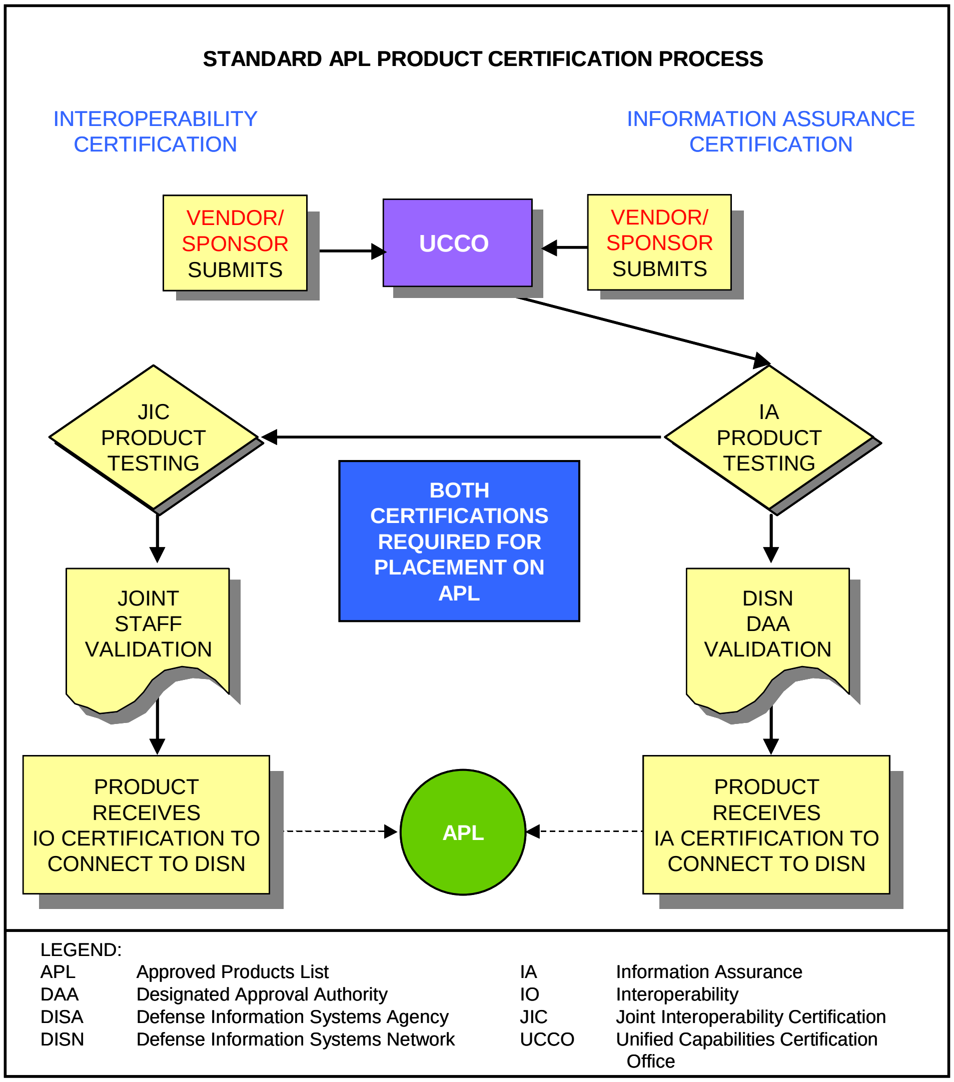

STANDARD APL PRODUCT CERTIFICATION PROCESS
INTEROPERABILITY CERTIFICATION
INFORMATION ASSURANCE CERTIFICATION
VENDOR/ SPONSOR SUBMITS
UCCO
VENDOR/ SPONSOR SUBMITS
JIC PRODUCT TESTING
IA PRODUCT TESTING
BOTH CERTIFICATIONS REQUIRED FOR PLACEMENT ON APL
JOINT STAFF VALIDATION
DISN DAA VALIDATION
PRODUCT RECEIVES IO CERTIFICATION TO CONNECT TO DISN
APL
PRODUCT RECEIVES IA CERTIFICATION TO CONNECT TO DISN
LEGEND:
APL Approved Products List
DAA Designated Approval Authority
DISA Defense Information Systems Agency
DISN Defense Information Systems Network
IA Information Assurance
IO Interoperability
JIC Joint Interoperability Certification
UCCO Unified Capabilities Certification Office

Figure 4.~~6~~5.3-1. Standard UC APL Product Certification Process

The following set of rules applies to the standard APL process:

1. Circuit-switched/TDM products will no longer be tested for APL status. Once their existing three year APL status expires they will be placed on the retired APL list. They will continue to be allowed to operate in the network. Exceptions to this policy will be submitted through the appropriate channels for ASD(NII) consideration. Circuit-switched/TDM product details are described in UCR 2008 for operational purposes only.

2.~~1.~~ ~~Circuit-switched/TDM products will no longer be tested for APL status, will be placed on the retired APL list, and will continue to be allowed to operate in the network.~~

A product enters the UC APL process by obtaining DoD Component sponsorship and providing both Interoperability and Information Assurance information as shown in Figure 4.~~6~~5.3-1.

~~2~~3. If a product successfully passed both Interoperability and Information Assurance portions of the testing, the product is placed on the UC APL. This listing is good for 3 years beginning on the day the UCCO announces the vendor's APL status, if no product changes are made. After the 3-year period has finished, products are placed on the "Retired List."

~~3~~4. If software and/or hardware changes are made, the product must be recertified for new purchases.

Procedures allow for changing the requirements a product must meet to become UC APL certified. Changes can come about because of the following:

- New or evolving technology changes
- Policy changes
- Changes in operational environment obviating the need for an existing requirement (e.g., Mfg., Discontinued)

When a requirement addition, change, or deletion has been approved on the date the UCR is signed, one of three dispositions will occur as follows:

1. The vendors will have 18 months to develop the requirement if it is new and not previously available. Vendors may provide it earlier.
2. If the requirement has been lessened, vendor compliance is immediate.
3. If warning of the requirements has been given before approval, the requirement compliance may be immediate.
4. If the requirement addresses a Critical or Major Information Assurance risk, compliance is immediate.
5. If the requirement is necessary for multivendor interoperability, compliance is immediate.

The 18-month period for development would apply to a new feature or a product not previously required, and the vendors did not have long-range knowledge of the requirement. New features or products in this version of the UCR are included in Table 4.~~6~~5.3-2, New Features and Products in UCR for Which 18-Month Rule Applies.

Section 5.8 Security Devices has been updated to add new Information Assurance products for Integrated Security Solutions, Information Assurance Tools, and Network Access Control. The 18-month rule does not apply to these.

A change sheet for the Section 5, Unified Capabilities Product Requirements, will identify which changes are subject to the 18-month rule and which ones are not.

Table 4.~~6~~5.3-2. New Features and Products in UCR 2010 for Which 18-Month Rule Applies

FEATURES	SECTION OF THE UCR
~~AS-SIP VTC Functionality~~	~~5.3.4.9.7.4~~
~~AS-SIP Generic End Instrument~~	~~5.3.2.6~~
~~V.150.1 Modem Relay Secure Telephone Support~~	~~5.3.2.21~~
~~AS-SIP TDM Gateway~~	~~5.3.2.7.4~~
~~AS-SIP IP Gateway~~	~~5.3.2.7.5~~
~~WAN SS~~Smartphone	~~5.3.2.8.4~~4.4.2.2.2
~~DSSS~~	~~6.2~~
Commercial Cost Avoidance	5.3.2.23
MD~~D~~SMCU	4.4.1.4
XMPP servers~~AS-SIP-Based Interfaces for Voicemail and Unified Messaging Systems~~	5.3.2.24
XMPP Client~~Information Assurance Requirements overlay for IM/Chat/Presence Awareness~~	5.7
Information Assurance Requirements overlay for IM/Chat/Presence Awareness~~IPv6 Profile 4.x Updates~~	5.3.5
~~SSH PKI Requirements~~	~~5.4~~
~~Deployed Tactical Radio~~	~~6.1.7~~
~~Army IA Products for which rqmts are provided~~	

A new APL process has been introduced called Fast Track (FT). The FT process is intended to expedite products onto the APL. The FT process is structured to deal with the fact that DoD sponsors have a need for products for which they have reasonably well-established requirements, and in some cases, test results. Yet these products do not appear in the UCR that is published on an annual basis. If the UC Steering Group agrees that new product categories and/or new products should be in the UCR, the DoD sponsors and vendors do not have to wait for the next UCR to get tested and placed on the APL. The APL testing can begin based on existing requirements that will be placed in the next version of the UCR. Products that are candidates for the FT process are as follows:

- Products that are within existing UCR product categories with well-established requirements, and in some cases, the existing requirements can be augmented by current UCR requirements

- Products that have existing test results that can be reused

- Products that are currently fielded and successfully performing from both an Interoperability and Information Assurance perspective in operational networks

- Products that should be added to the UCR per the UC Steering Group

Three categories of FT products are as follows:

1. Products within Current UCR Product Categories. Products that were tested by JITC before development of the product category or products that have existing requirements that are similar to those in the UCR that can be augmented with UCR requirements.

2. Operationally Validated. Products that are currently operating in DoD networks that have an IATO or ATO, are in compliance with appropriate STIGs, and are requesting APL status. Products may be end of life (i.e., retired APL status) or active (i.e., normal APL status).

3. New UCR Product Categories. Products that have existing DoD (non-UCR) requirements that can be used in the next version of the UCR and have been approved for the UCR by the UC Steering Group.

Additional and current information concerning the APL process can be obtained from the following online sources:

- UC APL Pages
  - UCCO Main Page: http://www.disa.mil/ucco/.
  - UCCO Policies and Procedures: This page contains important instructions and a breakdown of the UCCO Process (http://www.disa.mil/ucco/apl_process.html).
- ATC Pages
  - ATC Main Page: http://www.disa.mil/connect/.
  - ATC Policy, Guidance, and Procedures: http://www.disa.mil/connect/library/index.html.
  - ATC Process Overview: http://www.disa.mil/connect/overview/index.html.